Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset

Verena Zimmermann
Karen Renaud

Moving from a "Human-as-Problem" to a "Human-as-Solution" Cybersecurity Mindset

[1]Verena Zimmermann & [2]Karen Renaud
zimmermann@psychologie.tu-darmstadt.de, k.renaud@abertay.ac.uk
[1]TU Darmstadt, Darmstadt, Germany
[2]Abertay University, Dundee, UK & University of South Africa, Pretoria, South Africa

Abstract

Cybersecurity has gained prominence, with a number of widely publicised security incidents, hacking attacks and data breaches reaching the news over the last few years. The escalation in the numbers of cyber incidents shows no sign of abating, and it seems appropriate to take a look at the way cybersecurity is conceptualised and to consider whether there is a need for a mindset change.

To consider this question, we applied a "problematization" approach to assess current conceptualisations of the cybersecurity problem by government, industry and hackers. Our analysis revealed that individual human actors, in a variety of roles, are generally considered to be "a problem". We also discovered that deployed solutions primarily focus on preventing adverse events by building resistance: i.e. implementing new security layers and policies that control humans and constrain their problematic behaviours. In essence, this treats all humans in the system as if they might well be malicious actors, and the solutions are designed to prevent their ill-advised behaviours.

Given the continuing incidences of data breaches and successful hacks, it seems wise to rethink the *status quo* approach, which we refer to as *"Cybersecurity, Currently"*. In particular, we suggest that there is a need to reconsider the core assumptions and characterisations of the well-intentioned human's role in the cybersecurity socio-technical system. Treating everyone as a problem does not seem to work, given the current cyber security landscape.

Benefiting from research in other fields, we propose a new mindset i.e. *"Cybersecurity, Differently"*. This approach rests on recognition of the fact that the problem is actually the high complexity, interconnectedness and emergent qualities of socio-technical systems. The "differently" mindset acknowledges the well-intentioned human's ability to be an important contributor to organisational cybersecurity, as well as their potential to be "part of the solution" rather than "the problem". In essence, this new approach initially treats all humans in the system as if they are well-intentioned. The focus is on enhancing factors that contribute to positive outcomes and resilience. We conclude by proposing a set of key principles and, with the help of a prototypical fictional organisation, consider how this mindset could enhance and improve cybersecurity across the socio-technical system.

Keywords: Cybersecurity, Human's Role, Problematization, Socio-technical System

1. Introduction

Security incidents that endanger the confidentiality, integrity and availability of information abound, and are currently at an all-time high [1]. For example, IBM X-Force [2] tracked over 600 million leaked documents in 2015 and more than four billion in 2016. Other recently-reported breaches include Yahoo [3], LinkedIn [4], Last.fm [5], Equifax [6] and Marriott [7]. In October 2016, the Mirai botnet caused Internet-wide disruptions of major sites such as Etsy and Twitter [8]. Such events cost organisations and countries a great deal of money [9, 10], threaten critical infrastructures [11] and disrupt individuals' lives [12]. Many organisations are trying to find better ways to prevent incidents and halt the seemingly unhindered success rates of hackers [13]. As the whole world grapples with these issues [14], and cyber incidents continue to occur, there is a need to examine and question our existing mindset in terms of how we respond to this situation. Constructing a meta-view of cybersecurity and questioning the underlying assumptions might help generate new and helpful insights which can lead us down more effective paths, in terms of improved cybersecurity.

The aim of this research is to uncover characterisations of "the problem" in the cybersecurity arena. By so doing we want to reveal the underlying assumptions of this characterisation and to derive new reference points for improving cybersecurity. Our approach was governed by the research questions depicted in Figure 1, applying an interrogation technique called "problematizing" [15]. References to applicable sections and figures are contained within the diagram.

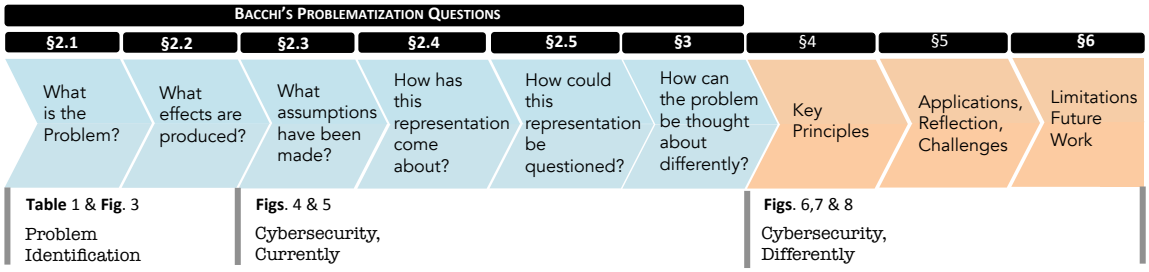

Figure 1: Problematizing Cybersecurity, and proposing 'Cybersecurity, Differently'

The problematization approach, detailed by Bacchi [16], is a way of questioning unstated and widely-accepted assumptions about a given field. It helps us to reconsider the veracity of existing characterisations of what is viewed as the underlying "problem". It is important to do this, because solutions are developed based on this conceptualisation of the problem space. Bacchi cites Foucault [17], who explains that problematization is concerned with how people govern themselves. He argues that we can strive to reveal truth about such governance by looking at general practice in an area. We can interrogate the area to find out what is *said* and what is *done* to reveal unstated yet commonly-held beliefs.

To illustrate the potential of this approach, consider knife crime. Shackle reported, in 2005 [18], that the WHO considered Glasgow to be the murder capital of Europe, with more than 1000 people being treated every year for serious facial trauma as a consequence. Solutions, up to that point, had focused on using the criminal justice system and active policing to address the issue [19]. Leyland and Dundas [20] pointed towards deprivation and inequalities to explain this phenomenon. Karen McCluskey from Strathclyde Police was the first to suggest that the problem was actually not a

criminal issue, but rather a public health issue [21]. Health issues are treated by curing them, not policing them, and the solutions McCluskey proposed aligned with the public health perspective. This new approach has paid off, dramatically reducing knife crime in Glasgow and across Scotland over the last decade [22, 23]. Re-problematizing changed perspectives about what the problem really was, and encouraged deployment of solutions that aligned with the new conceptualisation that led to a welcome reduction in knife crime.

In a field that is as complex and dynamic as cybersecurity, it is crucial for us to uncover and question what is viewed as the "problem" and not uncritically to accept existing wisdom in this respect.

Socio-technical systems, which is essentially what cyber systems are, are made up of multiple interconnected components, including human actors, technology and processes (Figure 2). On the component level, additional factors such as governance practices, organisational hierarchies and interactions between components come into play. All of these are further impacted by, and interact with, the outer environment and legislative constraints, and the result of such complexity is that it is almost impossible to predict outcomes with any degree of certainty. Systems outcomes are thus emergent.

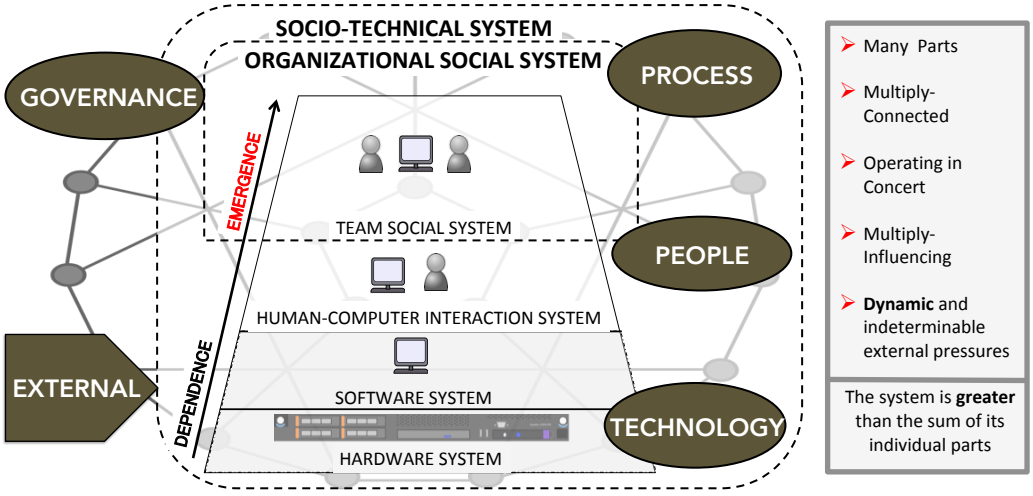

Figure 2: An overview of a typical socio-technical system (extended from [24]).

Our problematization process revealed an assumption that the individual human actor is generally considered to be "the problem" in the wider socio-technical cybersecurity system (Section 2). In Sections 2.5 and 3, we question this problem conceptualisation and review insights from the area of usable security and other disciplines, such as safety and management, that have brought about positive changes. Combining and adapting these interdisciplinary insights, we formulate new reference points and propose a different cybersecurity mindset, 'Cybersecurity, Differently' in Section 4. The approach is different from current efforts in that the human actors and their needs and limitations are not only considered in the system design, but the human is actually viewed as a *solution* rather than a *problem*. We describe examples and reflect on the challenges of achieving such a shift of mindset in security in Sections 5 and 6, and conclude in Section 7.

2. Problematization of cybersecurity

This section details our problematization process, which poses five of Bacchi's six questions [16], as depicted in Figure 1.

2.1. Question 1: What is the Problem?

We examined the cybersecurity-related public announcements and publications of government and industry. We also consider what hackers themselves have said about the problems they exploit. Details about how we extracted the government-, industry- and hacker-identified problems are provided in Appendix A.

2.1.1. Government-Identified Problems (Section Appendix A.1)

Many governments have published cybersecurity strategy policies, essentially encoding what government *says* and what they plan to *do*. Those in government who develop and write these policies do so based on their implicit understanding of the "problem" that the policy is formulated to address, whether or not their conceptualisation is explicitly stated or not.

Luiijf et al. [25] compared nineteen national cybersecurity strategies in 2013. In contrast to our approach, their analysis relied on the assumption of a common global set of threats and focused on differences in the aims and strategies formulated by governments to deal with these threats.

To contemplate governments' *problematizations* of cybersecurity, we had first to decide which countries' policies to analyse. A number of organisations publish Global Cybersecurity Index lists[1], but they differ in terms of what the index is based on, and countries appear in different positions on the lists.

We decided to focus on the cybersecurity policies published by the *Five Eyes* countries: Australia, Canada, the UK, the USA and New Zealand. This can be considered to be the world's most complete and comprehensive intelligence alliance [26].

2.1.2. Industry-Identified Problems (Section Appendix A.2)

We examined the complete security reports from the top five cybersecurity companies as ranked by eSecurity Planet[2]. Because most reports are released annually, we analysed the most recent freely available version. The companies' whose reports we analysed included: Cisco, Symantec, Palo Alto Networks, Check Point and Microsoft.

2.1.3. Hacker-Identified Problems (Section Appendix A.3)

How do hackers compromise systems? These are the "problems" that they exploit in order to breach system security. A few examples give us a sense of what they do and say. These were also analysed to isolate the problems revealed by their statements.

2.1.4. Summary: Outcome of the Problematization Process

The derived problems (P1 to P18) are shown in Tables 1 and 2, and depicted in Figure 3 within the socio-technical system.

[1] International Telecommunication Union (ITU) (`https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx`) NCSI `https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf`

[2] `https://www.esecurityplanet.com/products/top-cybersecurity-companies-2018.html`

	Problems	Government					H	Industry				
		AU	CA	UK	US	NZ		CP	CS	MS	PA	SY
Individual Level: Human	**P1:** Lack of Cyber Awareness, Knowledge and Skills	•	•	•		•	•	•	•	•	•	•
	P2: Lack of Accountability				•	•	•	•	•			
	P3: Lack of Policies & Compliance			•				•	•		•	
	P4: Not following Security Best Practice	•		•	•		•	•	•	•	•	•
	P5: Not Sharing Responsibility	•	•	•		•		•				
	P6: Malicious Employees	•							•			•
	P7: Cyber Criminals	•	•	•	•	•	•	•	•	•	•	•
Tech	**P8:** Software Vulnerabilities			•	•	•	•	•	•	•	•	•

Table 1: Individual and Technological Level Problems (AU=Australia; CA=Canada; UK=United Kingdom; US=United States; NZ=New Zealand; H=Hackers; CP=CheckPoint; CS=Cisco; MS=Microsoft; PA=Palo Alto; SY=Symantec)

The identified problems: lack of cyber knowledge, awareness and skills (P1), lack of accountability (P2), lack of policies and compliance (P3), lack of reporting (P18) as well as malicious activities by employees inside the organisation (P6) or cyber criminals outside the organisation (P7) concern the human actors, and their behaviours, on an individual level. Entities not wanting to take or share responsibility (P5) and shortcomings in following security best practices (P4) are located at the intersection of people, organisational processes and technology.

P7 and P8 concern activities of cyber criminals and software vulnerabilities, and are located at the intersection of people and technology, as software vulnerabilities are presumably caused, overlooked or not patched by software developers interacting with technology, and exploited by the cyber criminals. Thus, these problems again implicitly concern the human actor.

Some of the problems on an individual level are echoed on a societal or governmental level, e.g. a lack of individual cyber knowledge is mirrored by a general scarcity of cyber security professionals (P9), a lack of targeted research (P16) and a lack of local innovation (P11). Individual criminal activities are reflected in hostile nations' activities (P15) and challenges in detecting and prosecuting criminals (P10). In terms of the prevention and handling of cybersecurity incidents on a governmental level: a lack of leadership (P14), a lack of communication and collaboration (P12), a lack of trusted advice (P17) and problems in people reporting (P18) and appropriately responding to incidents (P13) are identified. The governance bubble influences and interacts with the core socio-technical system.

The challenges of detecting criminal activities (P10) and responding to incidents (P13) are located at the intersection between governance and technology. In organisations, the initial detection

	Problems	AU	CA	UK	US	NZ	**H**	CP	CS	MS	PA	SY
Societal Level: Governance	**P9:** Lack of Cyber Security Professionals		•	•		•			•			
	P10: Cyber Criminal Detection & Prosecution	•	•	•	•	•	•					
	P11: Insufficient Local Innovation in Cybersecurity	•	•	•	•							
	P12: Lack of Global Communication & Collaboration	•	•	•	•	•						
	P13: Inability to Defend/Respond	•	•	•	•	•						
	P14: Lack of Leadership	•	•	•	•	•						
	P15: Hostile Nations				•	•						
	P16: Lack of Targeted Research	•	•		•	•						
	P17: Lack of Trusted Advice		•			•						
	P18: Victims not reporting Cyber Incidents					•						

Table 2: Societal-Level Problems (AU=Australia; CA=Canada; UK=United Kingdom; US=United States; NZ=New Zealand; H=Hackers; CP=CheckPoint; CS=Cisco; MS=Microsoft; PA=Palo Alto; SY=Symantec)

and handling of abnormal or malicious activities depends largely on technological measures such as firewalls or intrusion detection systems that warn human operators and forward information for further processing.

To conclude, almost all of the identified issues in cybersecurity concern human actors in their various roles in some way, e.g. as software developers who create and maintain security-related technology, policy makers who introduce laws and standards, as well as employees and end users that make use of security-related technology while targeting other work-related or private goals. In the following, we will use the term "human actor" to acknowledge the variety of knowledge levels and roles of people in general, as compared to focusing solely on one particular role.

The problems at the governmental level are mainly concerned with preventing, controlling or responding to the problems at the individual level, such as lack of knowledge, skills and awareness, but also malicious behaviours. Even the problems that can be attributed to technology or processes are indirectly related to human behaviours. Human actors are using outdated technology, overlooking software vulnerabilities, falling for phishes, not following security policies and not sharing responsibility. The conclusion is that the human actor is viewed as the primary security risk and thus a "problem" to be dealt with.

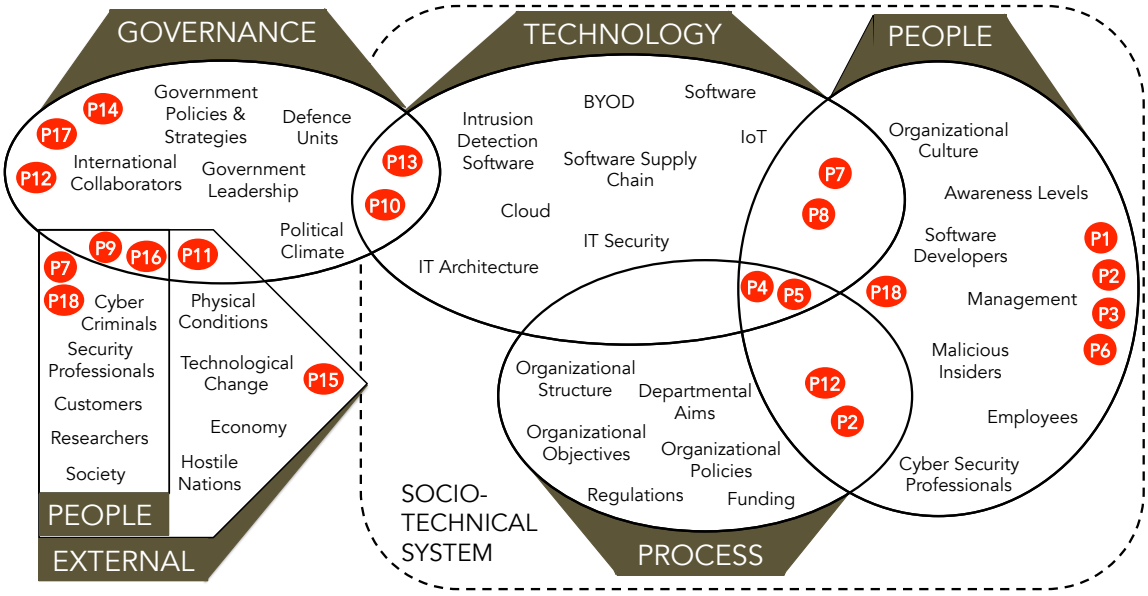

Figure 3: A socio-technical system diagram with the problems in Table 1 highlighted (The elements of each "bubble" are not meant to be wholly inclusive, but rather to be representative of the kinds of elements within each sector of the socio-technical system).

2.1.5. Related Research into the Human in the Cybersecurity Area

Because the focus of this research is on the role of the human actor in the socio-technical system, we provide a brief overview of human-centred research in the cybersecurity area. Research focusing on technical aspects is not reviewed.

A study carried out in 2017 analysed a decade's publications in major human-centred security conferences, in terms of whether they focused on the individual, on social aspects of human-centred security, or on their greater role in the socio-technical system [27]. The researchers discovered that the majority of papers focused on the individual, with a very small number focusing on social aspects or on the bigger picture. The primary focus was the human-computer interaction layer in Figure 2 i.e. the individual human actor's role in cybersecurity.

That being the focus, what aspects do academics study? Wood and Banks considered human error to be the most frequent cause of adverse incidents and "*a serious threat to the viability of computer-based systems, and thereby to the industrialised world at large*" [28, p.51]. Some say that the average computer user simply lacks knowledge and awareness of cybersecurity issues and of the secure behaviours they ought to be carrying out [29, 30]. Other researchers argue that a lack of knowledge is not the primary problem, but rather that users do not care about possible consequences, that they are unmotivated to take responsibility [31], or merely lazy. Herley [32] points out that the word "lazy" has traditionally been used to explain insecure end-user behaviours, although he disagrees with this characterisation.

Insecure behaviours, errors and the deployment of coping mechanisms have also been attributed to a mismatch between system design and human perception and cognition [28, 33, 34, 35, 36, 37]. Researchers in the relatively young field of usable security have focused on improving usability and coming up with solutions to design issues [38, 39].

In their seminal paper Whitten and Tygar [40], for example, identified usability issues as a primary reason for users not being able to encrypt emails. Disappointingly, more recent studies on encryption found that despite a great deal of research in the interim, people are still struggling to encrypt emails [41, 42].

Researchers have also investigated behaviours of the other humans in the socio-technical system, including cyber criminals [43, 44]. Some 16 years after Wood and Banks raised concerns about the computer user, Liginlal *et al.* [45] claimed that 67% of all analysed incidents were caused by human error, this being a significant precursor to privacy breaches in US firms.

This confirms that research is indeed being undertaken into many of the individual-related cyber problems. However, the topic of this paper: questioning the role of the human, when it comes to cybersecurity, has not yet been explored in any great depth.

2.2. Question 2: What Effects are Produced by this Representation?

Having identified the humans within the socio-technical system as a "problem to control", it is understandable that matching solutions to deal with the human would be deployed. Governments strategise, enact legislation and provide resources to drive change. On an operational level, the actions of organisations to address the "human as problem" include:

Exclude: Industry experts suggest excluding the human from the system as much as possible, suggesting automating of security processes or making them invisible. Cisco suggests that "*automation and intelligent tools [...] can help overcome skills and resource gaps.*" [p.10] [46]. A Verizon report puts it even more directly by stating: "*Automate anything you can as this reduces the human error associated with many breaches we see*" [p.36] [47]. Some academics agree with this sentiment [48].

Educate & Train: Standards bodies, such as NIST [49], academic researchers [50, 51] and industry [52, 46, 2, 53, 54, 47], highlight the necessity of training, manuals and security awareness campaigns. Consequently, many drives exist to increase security knowledge and awareness [55, 56]. Other approaches focus on making people care e.g. by inducing fear of negative consequences [57] or goal-setting [31].

Use Policies to Control & Constrain: Organisations implement a number of measures to control and prevent the insecure actions of human actors [58, 59]. The most widespread of these is the formulation and enforcement of security policies [29, 60, 61, 62]. The aim is to ensure that the human actor behaves securely, as instructed by the policies [46, 2, 63, 47, 64].

Conduct Root Cause Analyses: In many cases, in the aftermath of a new breach, a *root cause analysis* is carried out [65, 66, 67]. There is often a great deal of hindsight-enabled finger-pointing [68, 69, 70, 71, 72]. If there is sufficient public outrage, it is likely that someone will have to be held accountable and punished [73], before the media moves on to another story [74, 75, 76, 77]. The breached companies themselves sometimes terminate a single employee's employment, or at least pressure them to resign [78, 79, 80, 81], perhaps to show how serious they are about rooting out the negligent person behind the breach. Often, the response to adverse events is to re-train all employees, or to create more policies and processes to regulate human behaviours [82, 83].

In conclusion, the "human-as-problem" mindset manifests in measures that exclude the human or constrain human behaviour by requiring compliance with security policies. Efforts to increase awareness and knowledge are redoubled.

2.3. Question 3: What Assumptions have been Made?

To derive the assumptions behind the conceptualisations, we examine the identified problems and proposed solutions.

First, the outcome of our problem conceptualisation (Figure 3) indicates that the human in the system is the cause of cybersecurity errors and adverse events. We shall refer to this as **"*Human as Problem*"**.

Second, the review in Section 2.2 shows that the "human as problem" should be dealt with by: (1) excluding the human from the system [46, 47], (2) educating and training where exclusion is infeasible [52, 46, 2, 53, 54, 47], and (3) requiring compliance with security policies [46, 2, 63, 47, 84].

The underlying assumption is that adverse cyber events can be prevented by controlling and constraining the human actor's behaviour. We shall refer to this as **"*Exclude, Train, Constrain & Control*"**.

Third, the use of the aforementioned policy-based controls relies on the assumption that it is indeed possible to encapsulate all desirable security actions within policies and organisational processes. We shall refer to this as **"*Policy Adequacy*"**.

Fourth, building on the previous assumptions, it is concluded that the focus of cyber defence should be on preventing errors and adverse security events [28, 45]. This reveals an assumption that the absence of errors denotes the presence of security. We will refer to this as **"*Prevent Errors*"**

Fifth, when an adverse cyber event occurs, a "root cause" analysis should be carried out [85, 10] (Section 2.2). The underlying assumption is that a socio-technical system can be thought of as the sum of its parts and that incidents can be traced back to a single system component. "Fixing" this component should then prevent recurrences. We shall refer to this as **"*System Decomposability*"**.

Sixth, the next step, after the root cause analysis, should be to patch vulnerabilities, update or lock down devices or apply more automation and technology [47, 63, 54], in addition to tightening up security policies and measures to constrain employee behaviours [82, 83]. The assumption is essentially that *security-by-resistance* is the right way to go. We shall refer to this as **"*Resistance Stance*"**.

The different assumptions are depicted in Figure 4. These are essentially inter-dependent, and co-reliant.

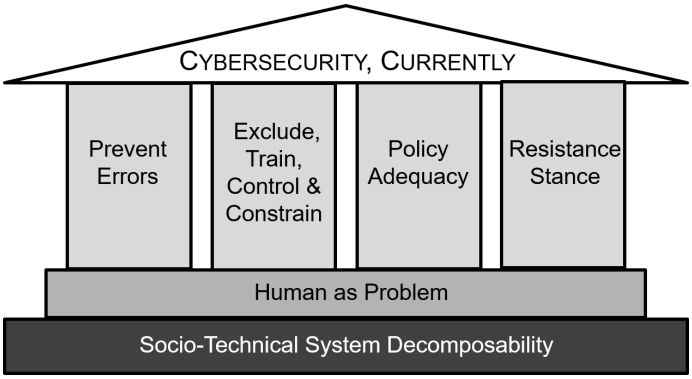

Figure 4: 'Cybersecurity, Currently' assumptions revealed by the problematization approach.

Figure 5 depicts the current 'Cybersecurity, Currently' mindset, based on our interpretation of the assumptions underlying identified problems. This figure depicts the three main socio-technical system components: people at the centre, using technology to carry out organisational functions, with processes encoding organisational means and methods of so doing. In this diagram, the mindset is outside-inwards: the human's behaviour is considered problematic and the organisation acts to

protect themselves from the consequences of their variable behaviours. Processes exist to impose control and are regularly reviewed in order to ensure that undesirable actions are curbed. Access to data and technology is severely constrained so as to prevent insecure actions.

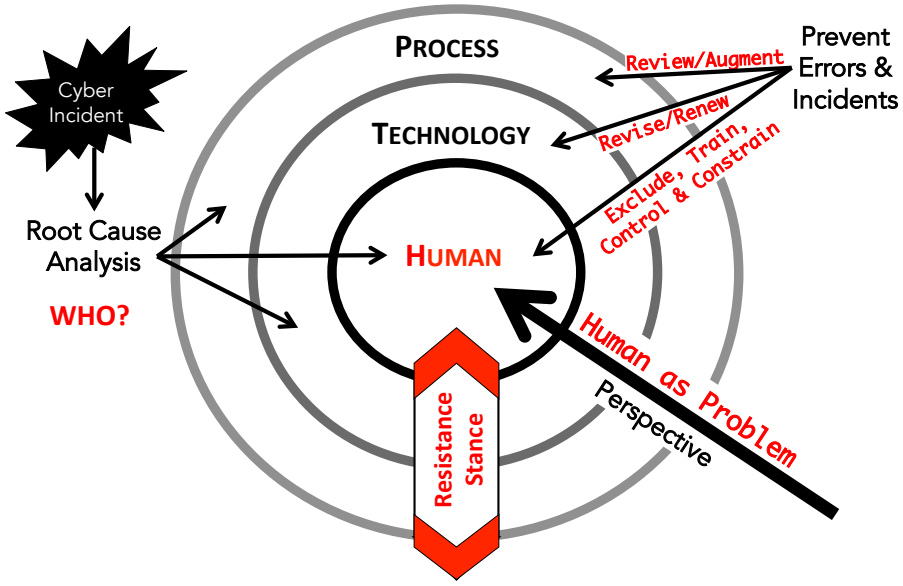

Figure 5: 'Cybersecurity, Currently': focus on controlling the human in the socio-technical system (Inspired by [86]).

2.4. Question 4: How has this Representation Come About?

A comprehensive discussion of this question is out of context for this paper. However, we do suggest an explanation for the core assumption about the human actor being the problem. When organisations initially started using computers, those responsible for computer security had two concerns: (1) physical security of the machines, which were usually housed in their own space, and (2) insiders accessing or destroying data, either deliberately or inadvertently. This led to an information security approach revolving around *governance, risk* and *compliance* (GRC) [87] and consequent control mechanisms such as policies, standards, and doctrines [88, 89]. This might have created a path that entrenched itself and informed all subsequent information security endeavours [90].

Anecdotally, the reasoning, currently, seems to be: (1) If a hacker exploits software vulnerabilities, that is the fault of the IT staff for not keeping the system patched and secure. (2) If someone falls for a phishing message, they did not pay enough attention. (3) If a breach occurs, it is possible that someone leaked their password or chose a weak one. In this way, every adverse event can be traced back to some human's failings or malicious behaviours and the human is perceived to be the one component that gets in the way of good security.

2.5. Question 5: How could this Representation be Questioned?

First, *Human as Problem*: The assumption that the human constitutes a problem to control is deeply rooted. Consider the Sony hack. Sony became aware of the presence and activity of

malware on their systems. Hackers stole personal information about employees, emails, executive salary details, and copies of unreleased Sony films [91]. Sony surmised that an IT administrator's password had been stolen, perhaps because he or she had been deceived by a phishing email. Arthur [83] reports that, *on the day after the Sony attack*, the FBI held information sessions during which employees were lectured about password "best practice" and spotting phishing attacks. Yet these employees did not open the door to the hackers. The hackers gained access directly via Sony's website using an exploit called SQL injection [92] and accessed the database that held all the user names and passwords stored in the clear. So, despite the fact that employees' behaviours did not trigger the breach, the immediate remediation incorrectly focused on their password choices and phish detection abilities, confirming unthinking attribution of a negative outcome to some human actor.

In reality, cyber incidents have multiple interacting causatives, and while the individual can indeed contribute, that is not the whole story. Socio-technical systems are complex, highly interactive and unpredictable, and adverse events have multiple contributing factors. Moreover, contrary to being the primary source of all problems, humans can actually be a vital player in *defending* against attacks [53]. Labelling human actors as "the problem" does not acknowledge their ability to detect anomalies and halt attacks.

Second, *Exclude, Train, Control & Constrain*: These remediations essentially remove responsibility from the human actor and do not permit them to be part of the solution. They are reduced to being rule followers; compliance becomes the mantra. Yet compliance only enhances security if the attackers do not innovate and change strategies, and only if the system is decomposable. Both of these assumptions, however, are unrealistic [93, 94] (see Figure 2).

Third, *Policy Adequacy*: Policies implement an *unexceptionalist approach* [95], applying the laws of the physical world to cyberspace. Yet cyberspace is not physical space. What is required is an *exceptionalist approach* that deals with cyberspace problems in a way that is better aligned with its idiosyncratic configuration and complexity.

Moreover, Cooper [93] points to a mismatch between defender (reactive) and hacker (proactive) strategies. Policies prevent individuals from countering innovative and evolving hacker tactics.

Fourth, *Prevent Errors*: The idea that errors can be prevented conflicts with the realities of the actual socio-technical system. Simply because errors are not making their presence felt can not automatically be interpreted as a sign that all is well.

Let us reconsider the Sony Hack. Subsequent investigations revealed widespread insecurities. Machines were not updated, people could install software downloaded from the Web, and passwords were being stored in plain text [96]. While the 2014 attack reached the media, this was not the first time Sony was hacked. In 2011, hackers had already breached their systems using SQL Injection [97]. This shows that Sony had systemic issues in 2011, and they were still there in 2014. These systemic flaws included inadequate governance & maintenance, and poor software engineering, among others. The huge Marriott data breach of 2018, too, was not the first successful hack — it was merely the last in a string of breaches [98]. In both these cases, no one noticed anything out of the ordinary, and the organisations were lulled into a false sense of security. A strategy that focuses solely on preventing and detecting errors is unlikely to detect ongoing security issues.

Fifth, *System Decomposability*: The Global State of Information Security Survey 2018 refers to "*an increasingly complex digital society*" [94]. The rising cyber interdependence of infrastructure networks is also acknowledged by the World Economic Forum [99] as: "*greater interdependence among different infrastructure networks is increasing the scope for systemic failures – whether from cyberattacks, software glitches, natural disasters or other causes – to cascade across networks and*

affect society in unanticipated ways" [p.7].

Root cause analyses, as a commonly deployed technique, do not acknowledge the multiple interactions and complexities of socio-technical systems. Looking for and remediating a single "root" suggests that it is indeed possible to isolate a single cause when the reality is that a multiplicity of causes often come together in an unpredictable fashion, to trigger an adverse event. A PwC report [94] acknowledges that "*organisations must dig deeper to uncover risks*" [p.10] that are inherent in today's socio-technical systems with emergent propensities.

Sixth, *Resistance Stance*: Many efforts to avoid cyber incidents focus on *hardening* the system. This can include adding more constraining rules to the policies [82].

The current successes of hacking attacks suggest that it is impossible entirely to avoid and resist cyber attacks, so we should rather turn our attention to more equally balancing resistance and efforts to build resilience [100]. Such resilience denotes the ability to recover to pre-event levels of functioning after a disturbance [101, 102].

Summary: It becomes clear, when one examines Figure 5, that the primary focus currently is on controlling the human actor, based on the assumption that their actions are problematic, and perhaps even malicious. This might be an effective strategy, except for the fact that the cyber arena is fluid and ever-changing. Hackers evolve their techniques and technology changes at an unprecedented rate [93]. Relying on policies to control human behaviour and thereby to prevent all errors does not acknowledge this reality. This situation is exacerbated by the fact that the usual response to adverse events is the enhancement of policies and reinforcement of compliance efforts. As the number of attacks escalate, it seems time to consider a different cybersecurity mindset.

3. *Question 6:* How can the Problem be thought about Differently?

We first provide an overview of insights gained from other disciplines that have taken a similar meta view of their practice, before returning to our cybersecurity theme:

Management: In the field of management, Hart [86] outlines the impacts of the kind of situation that is depicted in Figure 5. In particular, he explores the consequences when the focus is on controlling the human, and on ensuring that processes are followed to ensure best practice. He also speaks about reducing the human to a "rule follower", displacing responsibility from the human actor to the rules, and, beyond that, to the process formulator and policy writer [103]. Bourdieu [104] argues that this kind of displacement of responsibility to the policy makers drives a wedge between those who make policies, and practitioners who actually carry out the work. This could lead to practitioners disowning the problem.

The way humans are being "controlled" in cybersecurity is creating a situation where the human *becomes* a problem, because they are disempowered and marginalised by the controlling mindset: what systems theory calls a 'reinforcing loop'. Permitting people to take responsibility allows them to maximise their agency in terms of behaving to secure the organisation's devices and information. Moreover, Spector [105] finds that giving people control delivers high levels of job satisfaction and performance.

Military: In the military, Marquet [106], who was the captain of a nuclear-powered submarine, came to the realisation that he was creating a culture of following instead of individual leadership. Morale was low and serious mistakes were being made. He radically changed the way he ran his ship, and discovered that giving his crew ownership and control over problems, *at their own level of competence*, transformed his ship from the worst to the best in the fleet. This outcome was achieved by switching from controlling to trusting his junior officers and empowering them to make

the best decisions at their level of expertise. At the moment, this kind of trust is almost unheard of in cybersecurity practice.

Safety: This field delivers many valuable insights. Their beginnings were very similar to the way cybsersecurity works today. In the 1930s [107] safety equated to the achievement of zero accidents, incidents and failures. An accident was viewed as an event that "*invariably results from a completed sequence of factors — the last of these being the accident itself*" [107, p.13]. That is why this approach is often referred to as the "Domino Model" [108, p.64]. If an event, A, invariably led to an effect, B, the system could be considered to be bi-modal and easily decomposable. An accident analysis was conducted *post-hoc* with the help of accident reports and event trees. Heinrich concluded that 88% of accidents were directly caused by unsafe human acts [107, p.21], i.e. human error. This is similar to the current stance in cybersecurity where *post-hoc* analyses are carried out to identify single root causes, assuming that the underlying system is decomposable enough to support this.

Measures to prevent accidents in safety thus attempted either to find and eliminate causes [107, p.16], or to strengthen the barriers between the linear chain of events. Examples included technological automation, enforcing strict rules, mandating use of safety equipment, awareness posters and personnel adjustments, e.g., identifying and replacing the unreliable humans that caused the accidents, the "bad apples" [109, p.1]. This, too, is very similar to the way the cybersecurity field responds once they have identified the one human action that triggered an adverse event.

However, as the socio-technical safety systems developed and grew more complex over time, safety scientists realised that the previous approach was no longer fit-for-purpose. Many organisational and environmental factors and continuously changing system conditions impacted safety. Furthermore, the growing complexity of systems consisting of highly interconnected and tightly coupled components led to indeterminate behaviours [110]: System outcomes were emergent and often unpredictable [111], as are those in cybersecurity systems. An event, A, no longer necessarily led to an effect, B. Instead, an event, A, sometimes led to effect C or triggered a completely unexpected reaction.

The traditional safety approach also considered people to be the weak point and human behaviour a problem to be controlled [109]. Yet, an analysis revealed that the number of accidents was actually incredibly low given the complexity of the systems being studied. Examples of these studies include the US Air Traffic Control and US Navy nuclear aircraft carriers [112]. Analysing these so-called high-reliability organisations (HROs) [113], the researchers isolated particular factors that contributed to this high performance. These included high degrees of redundancy, flexibility, and deference to expertise. Employees were given an active role within the system and the freedom to react to changing system conditions. Furthermore, the organisations demonstrated a "culture" of high reliability. This was characterised by active seeking for, and elimination of threats, and a no-blame approach where employees could report errors without fearing negative consequences, thereby allowing the organisation to learn from errors [114]. Even though this initial research was descriptive in nature, and the factors unsuited to widespread application, the insights marked an important milestone towards the transition to "Safety, Differently", where humans were no longer viewed as "*a problem to control*" [115, p.13], but rather as "*a solution to harness*" [115, p.235].

These researchers and practitioners from different areas independently realised that they needed to change their paradigms, and each found ways of empowering the people in their organisations. The result, in all these cases, was more of the desired outcomes, not disaster.

Cybersecurity: Within the area of cybersecurity initial attempts were made to steer the field away from seeing the human agent the problem or "enemy" [38]. These focused on improving the

design of technology interfaces to enhance usability so as to align with human needs and limitations [38, 39]. For example, Adams and Sasse [38] urged interface designers to strive to understand the users' perspective and to design interfaces with the human in mind, not merely to consider them to be the cause of the problem. The relatively young field of "Usable Security" constitutes an important step towards empowering the human. Instead of excluding the human from the system, they argue that their needs and limitations should be given due consideration during system design.

Summary: The insights of these "human-as-solution" approaches [86, 106, 116] inform a new set of reference points. The novelty of the new approach lies in the fact that insights from various disciplines and approaches are combined and adapted to be applicable to the field of cybersecurity. The aim of this approach is to push the current efforts to no longer view the human as an "enemy" even further, and to foster the use of all available resources in socio-technical systems, including the human actor, to maintain and enhance cybersecurity. To fully develop the human actor's potential to be a contributor to cybersecurity, a shift in perspective is needed. We thus propose the 'Cybersecurity, Differently' mindset and describe its key principles next.

4. New Reference Points: Key Principles of 'Cybersecurity, Differently'

In the light of the ever increasing number of security incidents, we suggest adopting a new direction in the cybersecurity domain. An overview of the key principles of the new mindset that we call 'Cybersecurity, Differently' is depicted in Figure 6, highlighting how the key principles depend on, and reinforce, each other.

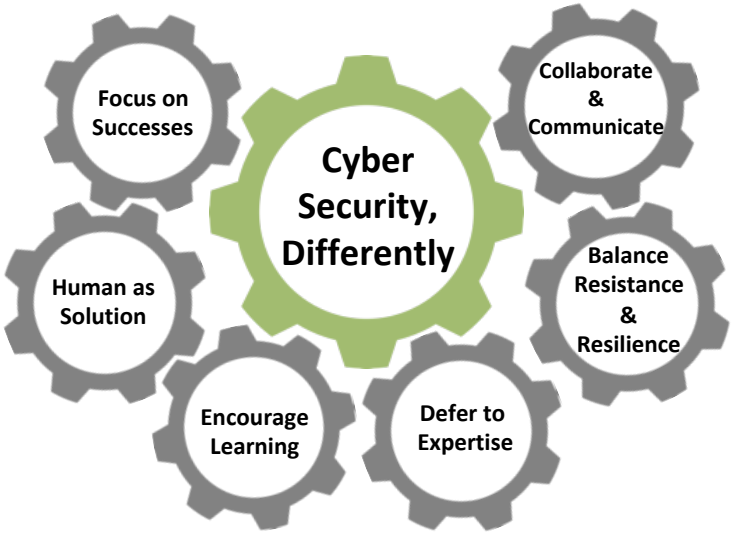

Figure 6: The key principles of 'Cybersecurity, Differently'.

'Cybersecurity, Differently' can be described as a new perspective on the human's role within complex socio-technical systems that incorporates insights from a number of related areas including

Safety [108, 115, 116, 113, 117], Medicine [118], Aviation [119], Management [86] and the Military [106].

Figure 7 shows how the human in 'Cybersecurity, Differently' can be at the centre and the starting point for maintaining and enhancing cybersecurity. In this diagram, the mindset direction is inside-outwards. In the following sections, we will explain how humans can be made part of the solution instead of being a problem to be controlled.

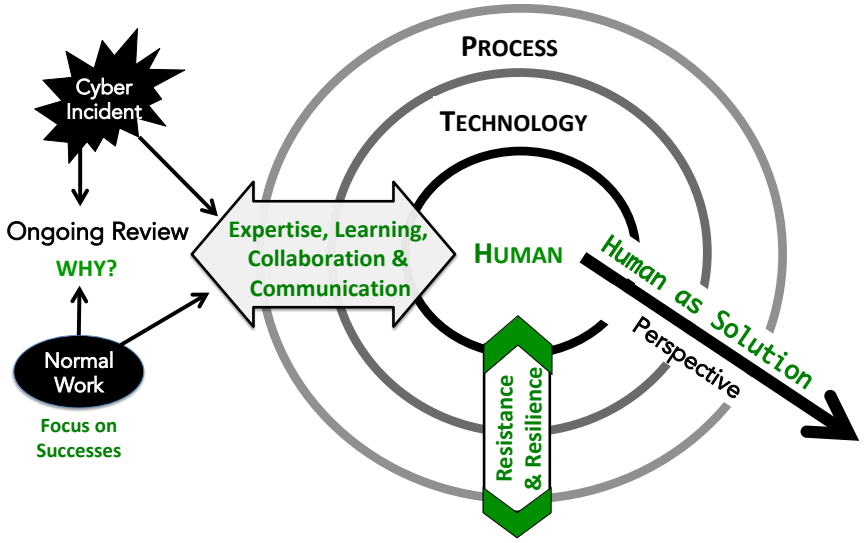

Figure 7: A new perspective: 'human-as-solution' i.e 'Cybersecurity, Differently' (Inspired by [86]).

4.1. Socio-Technical Systems — Decomposable vs. Emergent:

This assumption needs to be refuted at the outset, because it serves as foundation for the other assumptions enumerated in Section 2.3. While assuming decomposability is enticingly simple and supports the deployment of traditional tools, such as root cause analyses, it is also naïve in the face of cyber reality. As such, it can no longer be supported unquestioningly, given the complex, inter-dependent and evolving nature of cyber socio-technical systems.

In reality, the emergence of any behaviour, including errors or accidents, is a consequence of an interplay of different factors that interact and conspire together [102, p.13].

The WEF 2017 Global Risks Report found that cyber attacks, software glitches, and other factors could spark systemic failures that *"cascade across networks and affect society in unanticipated ways."* [99, p.5]. This suggests that the idea of flattening a socio-technical system and considering it the simple sum of its parts does not do the true situation justice. The system becomes more than the sum of its parts: creating interconnectedness, complexity and unpredictable, emergent outcomes. 'Cybersecurity, Differently' acknowledges the complexity, unpredictability and interconnected nature of socio-technical systems, with many dynamically interacting elements. Such elements include computers, networks, human actors in different roles and with different levels of security expertise, governance structures, operating systems, and the influences of the wider environment.

Adverse security events do need to be addressed and remedied. However, assuming decomposability and then focusing attention solely on one component of a complex socio-technical system is unrealistic, given the emergent nature of the underlying system's outcomes.

From this, we propose a more nuanced underlying assertion that:

→ **Today's socio-technical systems are complex and the outcomes thereof emergent, indeterminate and unpredictable**.

4.2. Human as Problem vs. Human as Solution:

'Cybersecurity, Differently' considers the human as integral and indispensible to the functioning of the socio-technical system as the facilitating technology. As such, they are indispensable contributors to security. We are not the first to suggest this kind of paradigm shift [120, 108, 86, 121, 106]; here we encapsulate the new mindset in a set of principles that apply to cyber security, extending the ideas proposed by other researchers [122, 123], who also make the case for applying insights from safety to cybersecurity.

Our proposed new mindset does not assume that humans do not make mistakes. Instead, it acknowledges that error and success are two sides of the same coin and that either label can only be assigned in hindsight [108]. Human performance variability might well contribute to errors, but, more importantly, also contributes to normal operation or success in the majority of instances [108]. Constraining humans or excluding them from the system means that we limit mistakes, but also that we limit all human agents' capacity to contribute actively to maintaining and improving security. Human actors should be allowed to participate in security efforts. Burkhead [124, p.114] notes that *"The detection and identification of incidents is heavily reliant on human reporting or human-assisted reporting"*.

In the cybersecurity arena, the Microsoft report recognises that humans are often called the weakest link in security but also that "*with the training and education they can also be the first line of defense*" [p.20] [53]. As an example they describe how employees spotting and reporting a suspicious mail can halt phishing attacks. A Verizon report [47] also finds that in a normal organisation 78% of employees do *not* fall for a single phish all year, showing how employees are often successful in spotting phishing emails. Because the focus is usually on errors, this important fact is not celebrated or highlighted. Moreover, by focusing on the negative aspects of human behaviour - errors - we demonise the human agents in the system and curtail their ability to play a positive role.

The mindset change we are advocating requires us to move on from focusing on the negative aspects of variability in human behaviour to realising that such variability is actually a strength that can be our greatest ally in cybersecurity. Moreover, embracing the human as the solution requires us to accept that the overwhelming majority of human actors within a socio-technical system have the intention to "do a good job" rather than to commit errors [116, p.99] (This excludes malicious human actors). This requires us to abandon knee-jerk negative characterisations, and rather to acknowledge that the majority of employees are trying to do their best in a complex and challenging environment.

Following this line of argument, we derive the first principle of 'Cybersecurity, Differently':

→ **Principle A: Acknowledge the Human Actor's Ability to be Part of the Solution**

4.3. Policy Adequacy vs. Deference to Expertise

"Deference to expertise" means that, regardless of hierarchy, the person with the highest level of expertise *for the task in hand* should be part of any decision process [115].

Cybersecurity expertise is important. However, human actors in socio-technical systems are not only IT specialists, administrators and software developers with high security expertise, but also all other human actors as "end users" with less expertise in security, but a great deal of expertise in their chosen profession. 'Cybersecurity, Differently' suggests that even human actors with minimal security expertise should be recognised as *task* experts. These are those who can best describe their tasks, their specific goals, the processes they engage in and identify the factors influencing these (e.g. time constraints). They should thus be actively involved in decision processes and the future development of cybersecurity mechanisms. Appropriate security measures should be derived jointly by security experts and the relevant task experts, instead of the former imposing security measures. Thus, the person with the highest level of expertise for a certain task, e.g. the IT staff in case of a security threat, should be involved in making decisions even though they might be ranked lower than the managers who make budgetary decisions. This helps to transfer security expertise to non-experts and align security processes with the human actors' context and tasks.

For example, Kirlappos [125] found that the main reason for non-compliance with security policies was that security conflicted with productivity. They concluded that the employees, as task experts, are the principal agents in deciding how security should be implemented in their specific contexts.

This new reference point is encapsulated in the next principle:

→ **Principle D: Defer to Expertise**

4.4. Exclude, Train, Constrain, Control vs. Encourage Learning, Communication and Collaboration:

We suggest that, when considering an adverse event, researchers and practitioners should focus on the *'why'*, instead of on the *'who'* [116]. Organisations should always act to learn from errors and encourage risk-free reporting rather than focusing on punishing individuals [116, 94]. All components of socio-technical systems can benefit from highlighting positive as well as negative events. To learn from events, and to be able to react quickly, reporting is essential. However, reporting is unlikely if employees or customers fear negative consequences such as blaming, shaming, financial loss, prosecution or job loss.

Safety scientists suggested establishing reporting systems that explicitly protect the individual [126] and focus on the *'why'*. Apart from errors or failures, the protected reporting of so-called "near misses" should be encouraged [119]. These are actions or situations that have the potential to go wrong but have not (yet) resulted in negative consequences. Similar approaches would also be feasible in the security area. Advantages include an extended quantitative database, the maintenance of a desirable level of alertness, and fostering insights into potentially insecure actions and situations [127].

Edmondson [128] explores the challenges of changing reference points in this way, and says this can be achieved by "*an environment of psychological safety that fosters open reporting, active questioning, and frequent sharing of insights and concerns*" [p.ii3]. Edmondson carried out a case study within a hospital and found that, by good leadership, learning was empowered and supported, changing the focus from error-detection and -prevention to learning and celebration of successes.

Furthermore, we suggest approaching cybersecurity incidents proactively, as compared to merely reacting to past cybersecurity incidents. Hudson [129] explains that a proactive approach, as opposed to a reactive approach, can engender high reliability in an organisation. Hollnagel [130] advises that the barriers to protect a system from threats must not become entirely reactive because safety cannot genuinely be improved by only looking into past events.

The proactive handling of, and learning from, incidents is summarised in the principle:

→ **Principle E: Encourage Learning**.

Learning from incidents and experiences can be fostered by communication and collaboration: There are two aspects to be considered here: (1) collaboration between humans and technology, and (2) communication between different human actors.

(1) Collaboration between Humans and Technology: Machines outperform humans in some areas and humans outperform machines in others. For example, humans are better at pattern recognition, improvisation, and decision-making with incomplete information. Machines, instead, are better at repeating tasks with high precision and speed or error-free retention of meaningless information. One approach to function allocation is HABA-MABA: *Humans are better at, Machines are better at* [131, 132] that highlights the fact that humans and machines have different strengths and weaknesses.

There is no suggestion that automation is always a bad idea, nor is it feasible to shift from "blaming" humans for errors to "blaming" technology or automation. Instead, we acknowledge that there are areas where automation is important, but there are also areas that cannot, or should not, be automated [119]. Instead of automating the human out of the system, 'Cybersecurity, Differently' suggests that every member of the wider socio-technical system be treated as an equal partner instead of mere substitution. It encourages the harnessing of both partners' strengths to create a sense of synergy or "team-work".

Using automation in a way that excludes the human from the system might lead to misunderstandings, security failures, or "automation surprises" [133] between those involved in an interaction. We therefore argue that when processes are automated, humans ought to be kept in the loop so that they can interact with the systems and extend their own expertise too [42].

(2) Communication between Human Actors: Communication between humans and technology and between different human actors is essential. It starts with the communication within work teams, but also between different organisational departments and with humans outside the organisation, such as customers or cooperating partners. PwC, for example, also calls for leaders in industry and governments to work together across national borders to identify and target cybersecurity threats and increase resilience [94]. The communication about cybersecurity should not only include experiences of handling threats and adverse events, but also the sharing of success stories that can be beneficial in deriving lessons for improving resilience.

From this, we derive the principle:

→ **Principle C: Communicate & Collaborate.**

4.5. Prevent Errors vs. Focus on Successes

The 'Cybersecurity, Differently' mindset focuses on successes and normal operation, the large majority of events that "go right" [108]. Similar to the safety area, the focus in security has long been on adverse events and human errors, which emerges from our review. Even though it is still important to analyse adverse events, we believe that organisations and researchers can learn a lot

by changing their perspective to also learning from successes and near misses [134]: what are people doing right that assures the security of an organisation's information?

In the large majority of cases, the same factors that contribute to an error or accident also contribute to the safe functioning of the system so that the label "error" or "success" can only be awarded in hindsight [102, p.13]. Dekker, for example, found that the same factors, e.g. work-arounds and deviations from procedures, in a few adverse events in the health care sector contributed to successful patient care in the large majority of cases [135]. It is thus important to evaluate both sides of the coin, negative and positive outcomes, before appropriate measures can be identified to enhance, facilitate, or communicate factors that contribute to cybersecurity.

The PwC report also suggests that organisations should "*pursue resilience as a path to rewards — not merely to avoid risk.*" ([94, p.12]). This indicates a call for a shift in focus from avoiding the negative to increasing positive outcomes. While this might not sound too different, the change in perspective influences the evaluation of outcomes, the measures undertaken to deal with them and also the type and proportion of analysed events. While incident or accident analysis conducted to avoid threats focus on the small percentage of adverse events, also analysing near misses and positive outcomes enlarges the database by including myriad "normal" events. This allows for statistical analyses often not possible with small numbers of negative incidents and a comparison of factors influencing positive vs. negative outcomes.

The MITRE Corporation, for example, embraced this idea [136] publishing success stories, and praising employees who spot phishing attacks and alert other employees.

This leads to the next principle:

→ **Principle F: Focus on Successes**

4.6. Resistance Stance vs. Balancing Resistance & Resilience

In a complex and emergent system, according to Hollnagel [102], threats are irregular, infrequent and unanticipated. They thus cannot be treated by focusing all efforts on resistance and building inflexible barriers. They require consideration of facilitating situations and conditions. This can be achieved by building resilience.

In this context, the term resilience can be defined as "*the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions*" [137]. It describes a system's capacity to deal with and recover from changing conditions and incidents.

According to Hollnagel [102], and as adapted to the security context, resilient systems should be able to:

- ***anticipate*** potential security incidents that could occur, and plan their responses beforehand.
- ***monitor*** past and present operating conditions and be alert to anomalies that could signal a problem or an attempted security attack.
- ***respond*** flexibly to an emerging situation when required. This includes having the situational awareness necessary to enable a response and the possibility to improvise.
- ***learn*** from, and reflect on, circumstances surrounding security incidents, with negative and positive outcomes alike, and being able to share conclusions in a no-blame fashion.

To build resilience, systems should be designed to keep the human in the loop, so that they are empowered to anticipate and detect anomalies, and also to respond to and remediate these [115, 138].

Consider an example from the health care sector from which elements could be easily transferred to security-related applications: Nemeth *et al.* [139] designed an infusion device control interface to act as a "team player". It provides the medic with operating history, current state and implications for the future. Contextual information, such as other therapeutic information or patient test results, are also provided to support a quick evaluation and recovery from unexpected conditions.

To conclude, humans must be given the flexibility to adapt their behaviour to the emergent behaviour of the underlying socio-technical system [102, p.13]. Such empowerment makes it more likely that they will be able to "re-stabilise" systems that have, or are being, compromised. In essence, resistance and resilience efforts should be balanced to ensure that the cyber risk is more effectively ameliorated.

The final principle is thus:

→ **Principle B: Balance Resistance & Resilience**

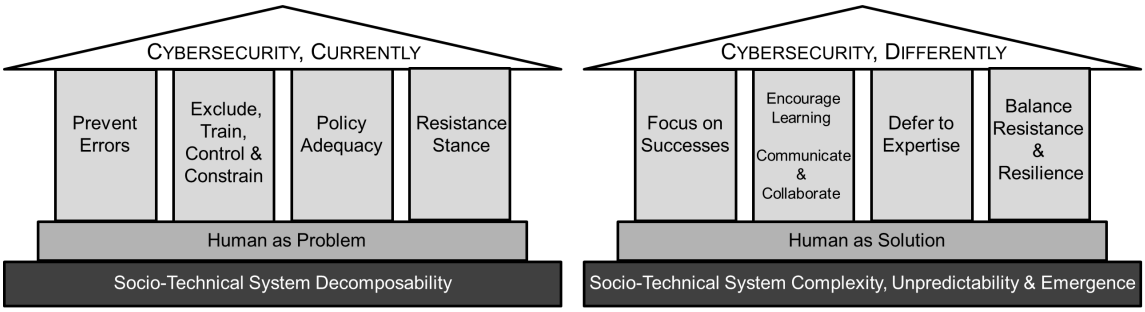

Figure 8: Contrasting 'Cybersecurity, Currently' assumptions with 'Cybersecurity, Differently' reference points.

Figure 8 contrasts the key principles that 'Cybersecurity, Differently' builds on, as compared to the current assumptions of 'Cybersecurity, Currently'.

5. Applications, Reflection & Challenges

In this section, we will describe how a fictional, exemplary organisation with a 'Cybersecurity, Currently', mindset might deal with named cybersecurity threats or incidents, as compared to an organisation with a 'Cybersecurity, Differently' mindset. We will point out the similarities and differences, including the benefits and the challenges that may arise from applying the new reference points. We contrast the two approaches based on the literature reviewed in this paper, but are aware that in practice there are many more variants of dealing with the named issues.

Imagine a medium-sized organisation named "EasyProject" (EP) that is mainly based in one country but acts globally and has industry partners and customers in different countries all over the world. It offers an online service that facilitates joint project management including the storage and joint editing of documents and timetables. They offer a free individual version as well as a subscription based version to companies.

Threat 1: Phishing Attacks

One of the most commonly identified threats, in many industry reports, is phishing [47, 140, 141, 142, 143, 46, 53], where an attacker tries to steal user credentials, e.g. by tricking employees into entering their credentials on a forged website. This is also an important threat to EP, because the credentials protect important and secret project documents created by its customers.

EasyProject, Currently: "EP, Currently" trains all its employees to raise security awareness and increase phish detection skills. Regular employees are trained separately from the security team and management to address role-specific aspects [46, 47]. The training focuses on the potential negative consequences of falling for a phish so as to increase the employees' motivation to pay attention to email messages. Further, to maintain a high level of awareness, the organisation regularly sends mock phishing emails to their own employees [53] using a tool similar to PhishMe [144] or Gophish [145]. The data of anyone clicking on the fake phish is collected. The person is redirected to a page to remind them of the need to take care, i.e. to seize the "teachable moment" and to deliver just-in-time re-training. To maximise resistance, and because the organisation's influence on other human actors outside the organisation (customers and partners) is limited "EP, Currently" implements a mechanism that automatically screens all emails and puts all suspicious emails into the Spam folder. This successfully prevents most phishing emails. However, some employees complain about missing emails from new business partners or customers, or having to check the Spam folder to detect falsely-junked emails.

EasyProject, Differently: Due to ongoing investigations of negative incidents as well as positive outcomes, EP discovered that 78% of human actors never click on phishing emails all year and that the number of people falling for a phish in a phishing campaign decreased from 11% to 4% [p.12] [47] (***Principle E & F***). Their analysis reveals that users are especially good at spotting phishing emails when it comes to issues of grammar or plausibility. However, they find the users have more trouble detecting tiny differences in embedded URLs. To address these cases, they use an algorithm to spot manipulations such as `Arnazon` instead of `Amazon` in the URL. Furthermore, technology is used to support the human: the parts of the URLs that they should pay attention to (e.g.[146]) or unprotected text entry fields are highlighted (e.g.[147]) to trigger caution and keep the human in the loop so they can spot and respond to anomalies (***Principle B***). In line with the HABA-MABA approach described above, human actors and machines can thus complement, instead of replacing, one another (***Principle C***). This way, even phishing emails overlooked by the technology are likely to be spotted and reported without over-constraining employees and customers. Reporting of phishing emails is encouraged and eased by implementing a button in the mail client to directly forward a suspicious mail to the security team (***Principle E***). Also, "EP, Differently" makes use of security awareness training that deliberately mingles employees from different departments to foster communication about security-related experiences (***Principle C***). People falling for a mock-phish in the training are not reported and the possibility to learn from the event is emphasised, The training also highlights the fact that security and other business goals such as cost and efficiency are equally important. The employees are made aware of the fact that they are the organisation's first line of defense. Everyone shares responsibility for cybersecurity.

Reflection & Challenges: Both "EP, Currently" and "EP, Differently" make use of training and technology to repel phishing attacks. This indicates that some current tactics are not a bad idea. Still, the way they are implemented in the two approaches is different: "EP, Currently" focuses on limiting human influence and preventing errors. This approach might force overly-constrained humans to look for work-arounds, such as using private email addresses or scanning the spam folder for missed emails, and accidentally clicking on a phishing email. "EP, Differently", on the other

hand, uses technology to support humans without constraining their tasks, such as interacting with new business partners and customers. "EP, Currently" trains groups separately and aims to increase security awareness through mock-phishing exercises. However, the approach might not only increase security but also induce negative feelings such as fear of being reported for falling for a fake phish, and shame for having to repeat training. "EP, Differently" aims to foster cross-organisational commitment to cybersecurity and free-flowing communication between departments. Training exercises are designed in a way that avoids reporting of individuals or inducing negative feelings, and instead to emphasise the possibility to learn (***Principle E***).

Threat 2: Weak Authentication

Many industry reports point to insecure authentication practices as an attack vector for organisations [140, 141].

EasyProject, Currently: To prevent weak passwords from being exploited, "EP, Currently" aims to increase their employees' and customers' password strength. They enforce new password policies mandating minimum strength and complexity requirements. They also disallow weak passwords [46] and require users to change their passwords every three months. Employee accounts require an additional authentication factor [46] to prevent stolen credentials being used. They issue mobile fingerprint readers, which generally work well. However, some have concerns about providing their biometric data and others forget to take the reader to meetings and are prevented from accessing important documents.

EasyProject, Differently: "EP, Differently" acknowledges the weak password problem, but also that weakness is not universal (***Principle F***). Acknowledging the users as experts (***Principle D***), they investigate the users' password behaviours and discover that some passwords are weak because of missing guidance, and that password strength often matches the value people attribute to the information being protected. They thus provide feedback on password strength and dynamic guidance on improving password strength [148]. Complexity requirements are not enforced [149] to improve memorability. Employees are not forced to change passwords to reduce the memorial burden [150]. Furthermore, free password manager subscriptions are issued to all staff. The technology is used to interact with and support the human actors rather than constrain and control them (***Principle C***).

For important accounts, a minimum password strength is required. For critical accounts, two factor authentication is implemented. The organisation examines actors' primary tasks and select token-based solutions that are privacy respecting. The second factor they choose is a Smartphone app that generates a one-time key on demand. Since people always carry their phones with them, they no longer get locked out of important accounts when away from their desks (***Principle D***).

Reflection & Challenges: Again, there are similarities: both perspectives aim to strengthen authentication. But there are also differences: "EP, Currently" does so by mandating a minimum password strength for all accounts. "EP, Differently" puts the human actor at the centre and analyses their needs and primary tasks before deciding on measures that balance security and usability. It aims to support the human in creating strong yet memorable passwords and provides tools to reduce memory load. However, "EP, Differently" also implements special measures for critical accounts. A challenge of their approach might arise from finding an appropriate balance between building resistance (e.g. minimum password strength or using two-factor authentication) and giving users flexibility and freedom.

Threat 3: User credentials leaked

An EP employee discovers that user credentials have been leaked. It is not yet clear how it happened or how many customers are affected. However, the organisation now needs to deal with this unfortunate situation.

EasyProject, Currently: "EP, Currently" conducts a root cause analysis to identify who caused the leak. The leak is traced back to a member of the security department whose computer was compromised by malware exploiting a software vulnerability. The questioning of the security team member reveals that the employee's email account was also used for private emails and that the employee sometimes used his own USB stick to take documents home to work on. This is recorded in the employee's personal file as a discplinary offence. "EP, Currently" notifies the customers whose credentials were leaked and instructs them to change their passwords. To prevent a re-occurrence, security team members are retrained in following security best practice. New security policies and controls are introduced to prevent private use of employee business email accounts. All USB ports are disabled across the organisation's computers.

EasyProject, Differently: "EP, Differently" also conducts an analysis to identify the factors that contributed to the leak. They trace the leak back to malware that compromised a security team member's computer. To identify and compare the factors contributing to both adverse events and positive outcomes a number of employees are interviewed confidentially about their security practices (***Principles A & F***). The investigation reveals technological, human and organisational factors that contributed to the emergence of the incident. A software vulnerability was identified. Furthermore, it became clear that many employees were using their work email address for private purposes as the organisation's firewall blocked other email service providers. This prevented employees from checking their private email at work.

USB sticks were being used to take organisational data home to work on. Allowing staff remotely and securely to access the organisation's intranet was not yet widely available. Organisational pressure to react to IT incidents quickly and after hours, however, required employees to be able to access data from home. While these practices enabled employees to fulfil their tasks (***Principles A & F***), it also contributed to the leakage of data in one case. Also, the finding related to email helped the organisation to understand employees' needs as work and private lives increasingly become interwoven.

In responding to the incident "EP, Differently" does the following: (1) Inform all customers of the leakage, whether their credentials were leaked or not. The notification explained the situation, possible consequences and measures undertaken to remediate. Support for changing passwords and checking for potential misuse of the credentials is offered. (2) Inform all employees about the incident, the interacting factors contributing to it and the possibility it offered to learn, without pointing at a single human or department (***Principle B, C & E***). (3) Implement changes based on the findings to balance employees' needs and security (***Principle A***): e.g., make secure remote access available to facilitate working from home and to remove the need to use USB sticks, and allow users to link their private with their work email account to avoid the need for workarounds.

Reflection & Challenges: In both cases, an investigation is carried out and reveals similar causatives. However, "EP, Differently" not only focuses on the incident, but also on normal work, and acknowledges human performance variability. This helps to uncover underlying factors and potential remediatons. Furthermore, another focus is on sharing information transparently and encouraging future reporting by using the adverse event as a learning opportunity. Challenges of the 'Cybersecurity, Differently' approach in terms of reporting and learning arise when legal aspects come into play that require de-anonymisation and accountability.

6. Limitations & Future Work

Malicious Behaviour: We need to emphasise that the focus of this research and the "*Security, Differently*" approach is on the well-intended human actor, the software developer who aims to create secure and usable software, the employee who aims to do a good job, and the end user who aims to use services and products as intended. However, the cybersecurity socio-technical system also includes malicious actors. These can be insiders or outsiders aiming to compromise systems for financial or political reasons. In one of the examples provided above, data was leaked by accident. However, it could also have been leaked deliberately and many of the threats described above, such as weak authentication, are only threats because they are exploited by cyber criminals. Malicious behaviours and cyber criminals are mentioned by all analysed government policies and industry reports. It only takes a single malicious human to compromise a system, so this small group cannot be neglected. This is probably why most research has thus far focused on resistance, as described in Section 2.

The assumption driving 'Cybersecurity, Differently', however, is that the overwhelming majority of human actors aim to do a good job. Thus, we assume that the majority of employees are well-intended, until they betray that trust. This is contrary to the current situation where controls treat everyone as malicious, on the assumption that they are likely to compromise security if allowed any leeway. On the one hand, giving employees more freedom and responsibility, as suggested by 'Cybersecurity, Differently', might make it easier for malicious parties to carry out their activities. Yet treating all employees as potentially malicious actors, based on a minority being malicious, is what we are arguing against.

Mistrusting, constraining and controlling the majority of employees or customers on the assumption that they might be malicious is likely to foster a destructive organisational culture, lead to employees eschewing responsibility for cybersecurity, to search for "non-compliant" workarounds, or even triggering malicious activities as reactions to a general culture of mistrust. In contrast, an organisational culture, as proposed by 'Cybersecurity, Differently', where people willingly share responsibility for cybersecurity and are constantly monitoring the system, might not hinder all malicious activities but at least contribute towards early detection or prevention of attacks. As stated by the Microsoft report [53] employees can not only be the weakest link but also *"the first line of defence. An employee that spots and reports a suspicious email could head off an extensive phishing campaign. And employees that note unexpected latency in systems can set off investigations that uncover lurking threat actors.*" [p.20]. 'Cybersecurity, Differently' does not suggest that all defence mechanisms be rendered inoperative, but to balance resistance and resilience. That is, to treat the human actor as an ally in preventing and detecting malicious actors instead of treating all human actors with suspicion. Still, the change in the mindset and organisational culture suggested by 'Cybersecurity, Differently' cannot be accomplished overnight. Future research is needed on how to move humans incrementally into the proposed state and mindset. Further, finding a suitable balance between preventing and detecting malicious actors, and fostering well-intended, positive outcomes, constitutes another direction for future research.

Implementation and evaluation of practical measures: With the help of a fictional organisation we described the handling of certain threats and incidents according to the 'Cybersecurity, Differently' mindset to achieve our vision in Section 5. Even though the examples are based on real cases and suggestions from research and industry, they are essentially still only examples. A direction for future research is the development, implementation and evaluation of concrete measures that contribute to the vision of 'Cybersecurity, Differently'. This includes measures that target single aspects, such as interface design, according to the principles of resilience engineering, but also

measures covering multiple aspects, e.g. measures fostering changes in the organisational culture. Apart from the direct and short-term effects of these measures, studies analysing long-term effects, side effects or effects on distant parts of the socio-technical system would be of interest.

The Problematization Approach: Within the problematization approach described in Section 2, we analysed a variety of documents, including cybersecurity policies of different states, security reports of different organisations and hacker-self-reports. However, the analysis was not exhaustive and might benefit from applying the approach to other documents and contexts. Apart from this, for the scope of this paper, only the foreword and the executive summary of the policies were scrutinised. A complete analysis might further extend the scope of the research and complement the "big picture".

7. Conclusion & Summary

The research reported in this paper analysed a variety of cybersecurity-related documents from governments, industry and hackers using a problematization approach. This approach is used to reveal underlying assumptions in a certain field based on the idea that if such assumptions are incomplete, incorrect or unfounded, the solutions, too, will be mismatched and ineffective. Our analysis revealed that many of the 'problems' identified in cybersecurity are directly or indirectly attributed to the human actor, e.g. software developers, employees or end users. Based on this "human-as-problem" mindset, human actors are currently excluded, trained, constrained and controlled to comply with security policies, and to increase resistance. This is the *"Cybersecurity, Currently"* approach.

Building on combined insights from other disciplines, such as management and safety, we question the current viewpoint and aim to build on earlier efforts in the field of usable security. We propose a shift from seeing the human as a problem, to appreciating the human actor's potential to contribute to success. This "human-as-solution" mindset, where the human's role is newly envisioned, is referred to as *"Cybersecurity, Differently"*. The new approach acknowledges the complexity and interconnectedness of today's cybersecurity systems, within which outcomes are emergent. It views the human as having the potential to be a contributor to success, a "solution", within the wider socio-technical system. The new approach encourages deference to expertise, flexibility, and learning from positive as well as negative outcomes. It engenders communication and collaboration, and relies on balancing resistance and resilience to enhance cybersecurity.

We are aware that this kind of shift in perspective will not be trivial to achieve. Challenges remain, e.g. in the detection and handling of malicious agents' activities. 'Cybersecurity, Differently' focuses on the large majority of well-intended human actors and argues against treating them as malicious on account of a very small minority of internal malicious actors. This mindset shift aims to increase individual responsibility and levels of cybersecurity awareness. We hope thereby to decrease or at least more quickly detect anomalies and malicious activities. However, future work is clearly needed to find a balance between avoiding malicious and fostering well-intended behaviours.

Our principles are still preliminary and further research is needed to develop, implement and evaluate concrete measures that can incrementally contribute to the shift towards a new mindset. Our objective with this paper is to spark interest in the vision of 'Cybersecurity, Differently', as a first step towards a new era in cybersecurity research and practice.

Acknowledgement

This research work has been funded by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity.

References

[1] Kroll.com, Global Fraud & Risk Report, Forging New Paths in Times of Uncertainty, https://www.kroll.com/en-us/global-fraud-and-risk-report-2018 10th Annual Edition 2017/18 (Accessed 5 January 2019) (2018).

[2] M. Alvarez, N. Bradley, P. Cobb, S. Craig, R. Iffert, L. Kessem, J. Kravitz, D. McMillen, S. Moore, IBM X-Force Threat Intelligence Index 2017 The Year of the Mega Breach, IBM Security March (2017) 1–30.

[3] E. Weise, It's new and it's bad: Yahoo discloses 1B account breach, 14 December, https://www.usatoday.com/story/tech/news/2016/12/14/yahoo-discloses-likely-new-1-billion-account-breach/95443510/ (Accessed 5 January 2019) (2016).

[4] E. Schuman, LinkedIn's disturbing breach notice, 01 June, https://www.computerworld.com/article/3077478/security/linkedin-s-disturbing-breach-notice.html Computerworld Jun 1 (Accessed 5 January 2019) (2016).

[5] J. Mannes, 43 Million Passwords Hacked in Last.fm Breach, 02 September, https://techcrunch.com/2016/09/01/43-million-passwords-hacked-in-last-fm-breach/ (Accessed 5 January 2019) (2016).

[6] K. Yurieff, Equifax data breach: What you need to know, 10 September, http://money.cnn.com/2017/09/08/technology/equifax-hack-qa/index.html (Accessed 5 January 2019) (2017).

[7] Forbes, Marriott breach: Starwood hacker gains access to 500 million customer records, 30 November, https://www.forbes.com/sites/forrester/2018/11/30/marriot-breach-starwoods-hacker-tier-rewards-millions-of-customer-records/#3f90b0245703 (Accessed 5 January 2019) (2018).

[8] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, et al., Understanding the Mirai botnet, in: 26th USENIX Security Symposium (USENIX Security 17), USENIX Association, 2017, pp. 1092–1110.

[9] Z. Rodionova, Cyber security report: Hacking attacks on UK businesses cost investors £42bn, 12 April, https://www.independent.co.uk/news/business/news/cyber-hacking-attack-cost-uk-business-investors-ftse-companies-lose-120-million-a7678921.html (Accessed 15 December 2018) (2017).

[10] Ponemon Institute, 2017 Cost of Data Breach Study: Global Overview, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN& (Accessed 15 December 2018) (2017).

[11] ICS-CERT, Alert (IR-ALERT-H-16-056-01):Cyber-Attack Against Ukrainian Critical Infrastructure, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 (Accessed 5 January 2019) (2016).

[12] J. Fae, Fraudsters are becoming more sophisticated in the ways they con you out of your precious savings, 4 January, https://www.independent.co.uk/news/long_reads/fraud-victims-age-young-old-elderly-lose-money-vulnerable-financial-crime-identity-a8134516.html (Accessed 5 January 2019) (2018).

[13] K. J. McAlpine, Patch fixes won't stop massive data breaches. what will?, 4 December, https://www.bu.edu/research/articles/marriott-data-breach/ (Accessed 5 January 2019) (2018).

[14] R. Sobers, 60 must-know cybersecurity statistics for 2018, 18 May, https://www.varonis.com/blog/cybersecurity-statistics/ (Accessed 7 January 2019) (2018).

[15] C. Bacchi, Why study problematizations? Making politics visible, Open Journal of Political Science 2 (1) (2012) 1–8.

[16] C. Bacchi, Analysing policy, Pearson Higher Education AU, 2009.

[17] M. Foucault, Questions of method, in: The Foucault effect: Studies in governmentality, University of Chicago Press, 1991, pp. 73–86.

[18] S. Shackle, Should we treat crime as something to be cured rather than punished?, 24 July, https://www.theguardian.com/news/2018/jul/24/violent-crime-cured-rather-than-punished-scottish-violence-reduction-unit (Accessed 5 January 2019) (2018).

[19] BBC, Homicide rate hits 10-year high, 14 December, http://news.bbc.co.uk/1/hi/scotland/4527570.stm (Accessed 5 January 2019) (2005).

[20] A. H. Leyland, R. Dundas, The social patterning of deaths due to assault in Scotland, 1980–2005: Population-based study, Journal of Epidemiology & Community Health 64 (5) (2010) 432–439.

[21] M. Bulman, Woman who helped dramatically reduce youth murders in Scotland urges London to treat violence as a 'disease', 5 April, https://www.independent.co.uk/news/uk/home-news/london-gang-violence-youth-murders-name-scotland-public-health-disease-crime-reduction-a8288596.html (Accessed 5 January 2019) (2018).

[22] P. O'Hare, From murder capital of Europe to role model for London, 19 September, https://www.bbc.co.uk/news/uk-scotland-45572691(Accessed 5 January 2019) (2018).

[23] The Economist, As knife crime rises in England, police look to Glasgow, 23 August, https://www.economist.com/britain/2018/08/23/as-knife-crime-rises-in-england-police-look-to-glasgow(Accessed 5 January 2019) (2018).

[24] C. Lebeuf, M.-A. Storey, A. Zagalsky, How software developers mitigate collaboration friction with chatbots, in: 20th ACM conference on Computer-Supported Cooperative Work and Social Computing (CSCW '17), 2017.

[25] E. Luiijf, K. Besseling, P. De Graaf, Nineteen national cyber security strategies, International Journal of Critical Infrastructures 6 9 (1-2) (2013) 3–31.

[26] J. V. Tossini, The Five Eyes – The Intelligence Alliance of the Anglosphere, 14 November, https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/ (Accessed 5 January 2019) (2017).

[27] K. Renaud, S. Flowerday, Contemplating human-centred security & privacy research: Suggesting future directions, Journal of Information Security and Applications 34 (2017) 76–81.

[28] C. C. Wood, W. W. Banks Jr, Human error: an overlooked but significant information security problem, Computers & Security 12 (1) (1993) 51–60.

[29] E. Kritzinger, S. H. von Solms, Cyber security for home users: A new way of protection through awareness enforcement, Computers & Security 29 (8) (2010) 840–847.

[30] S. Kraemer, P. Carayon, Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists, Applied Ergonomics 38 (2) (2007) 143–154.

[31] K. Thomson, J. Van Niekerk, Combating information security apathy by encouraging prosocial organisational behaviour, Information Management & Computer Security 20 (1) (2012) 39–46.

[32] C. Herley, So long, and no thanks for the externalities: the rational rejection of security advice by users, in: Proceedings of the 2009 Workshop on New Security Paradigms Workshop, ACM, 2009, pp. 133–144.

[33] S. Chiasson, P. C. Van Oorschot, Quantifying the security advantage of password expiration policies, Designs, Codes and Cryptography 77 (2-3) (2015) 401–408.

[34] C. Herley, P. Van Oorschot, A research agenda acknowledging the persistence of passwords, IEEE Security & Privacy 10 (1) (2012) 28–36.

[35] K. Renaud, M. Volkamer, A. Renkema-Padmos, Why doesn't Jane protect her privacy?, in: International Symposium on Privacy Enhancing Technologies Symposium, Springer, 2014, pp. 244–262.

[36] C. Posey, T. L. Roberts, P. B. Lowry, R. T. Hightower, Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders, Information & Management 51 (5) (2014) 551–567.

[37] M. A. Sasse, S. Brostoff, D. Weirich, Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security, BT technology journal 19 (3) (2001) 122–131.

[38] A. Adams, M. A. Sasse, Users are not the enemy, Communications of the ACM 42 (12) (1999) 40–46.

[39] D. Balfanz, G. Durfee, D. K. Smetters, R. E. Grinter, In search of usable security: Five lessons from the field, IEEE Security & Privacy 2 (5) (2004) 19–24.

[40] A. Whitten, J. D. Tygar, Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0, in: USENIX Security Symposium, Vol. 348, 1999, pp. 169–184.

[41] S. Ruoti, N. Kim, B. Burgon, T. Van Der Horst, K. Seamons, Confused Johnny: when automatic encryption leads to confusion and mistakes, in: Proceedings of the Ninth Symposium on Usable Privacy and Security, ACM, 2013, pp. 5–12.

[42] S. Ruoti, J. Andersen, S. Heidbrink, M. O'Neill, E. Vaziripour, J. Wu, D. Zappala, K. Seamons, We're on the same page: A usability study of secure email using pairs of novice users, in: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, ACM, 2016, pp. 4298–4308.

[43] H. Park, S. Cho, H.-C. Kwon, Cyber forensics ontology for cyber criminal investigation, in: International Conference on Forensics in Telecommunications, Information, and Multimedia, Springer, 2009, pp. 160–165.

[44] R. Smith, P. Grabosky, G. Urbas, Cyber criminals on trial, Criminal Justice Matters 58 (1) (2004) 22–23.

[45] D. Liginlal, I. Sim, L. Khansa, How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management, Computers & Security 28 (3-4) (2009) 215–228.

[46] Cisco, Cisco 2018 annual cybersecurity report, `https://www.cisco.com/c/en/us/products/security/security-reports.html` (Accessed 05/01/2019) (2018).

[47] S. Widup, M. Spitler, D. Hylender, G. Bassett, 2018 Verizon Data Breach Investigations Report, `http://www.verizonenterprise.com/de/DBIR/` (Accessed 5 January 2019) (2018).

[48] S. Vidyaraman, M. Chandrasekaran, S. Upadhyaya, Position: The user is the enemy, in: Proceedings of the 2007 Workshop on New Security Paradigms, NSPW '07, ACM, New York, NY, USA, 2008, pp. 75–80. doi:10.1145/1600176.1600189.

[49] National Institute of Standards and Technology, Cybersecurity Framework , `https://www.nist.gov/cyberframework` (Accessed 5 January 2019) (2014).

[50] A. McIlwraith, Information Security and Employee Behaviour: How to Reduce Risk through Employee Education, Training and Awareness, Routledge, Oxon, 2016.

[51] K. Øien, S. Massaiu, R. Tinmannsvik, F. Størseth, Development of early warning indicators based on resilience engineering, in: Submitted to PSAM10, International Probabilistic Safety Assessment and Management Conference, 2010, pp. 7–11.

[52] Check Point Software Technologies Ltd, 2018 security report - welcome to the future of cyber security, `https://www.checkpoint.com/downloads/product-related/report/2018-security-report.pdf` (Accessed 5 January 2019) (2018).

[53] A. Hatekar, et al., Microsoft security intelligence report - volume 23, `https://info.microsoft.com/rs/157-gqe-382/images/en-us_cntnt-ebook-sir-volume-23_march2018.pdf` (Accessed 5 January 2019) (2018).

[54] Symantec Corporation, Internet security threat report - volume 23, https://www.symantec.com/security-center/threat-report (Accessed 5 January 2019) (04 2018).

[55] B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, MIS Quarterly 34 (3) (2010) 523–548.

[56] M. T. Siponen, A conceptual foundation for organizational information security awareness, Information Management & Computer Security 8 (1) (2000) 31–41.

[57] A. Vance, D. Eargle, K. Ouimet, D. Straub, Enhancing password security through interactive fear appeals: A web-based field experiment, in: 46th Hawaii International Conference on System Sciences (HICSS), IEEE, 2013, pp. 2988–2997.

[58] A. D. Rayome, Report: Negligent employees are no. 1 cause of cybersecurity breaches at SMBs, 19 September, https://www.techrepublic.com/article/report-negligent-employees-are-no-1-cause-of-cybersecurity-breaches-at-smbs/ (Accessed 5 January 2019) (2017).

[59] W. R. Daugherty, Human error is to blame for most breaches, 6 June, http://www.cybersecuritytrend.com/topics/cyber-security/articles/421821-human-error-to-blame-most-breaches.htm (Accessed 5 January 2019) (2016).

[60] M. Siponen, S. Pahnila, M. A. Mahmood, Compliance with information security policies: An empirical investigation, Computer 43 (2) (2010) 64–71.

[61] W. E. Sobel, G. Vogel, B. McCorkendale, Enforcement of compliance with network security policies, 24/07/2007, US Patent 7,249,187 (2007).

[62] S. Bauer, E. W. Bernroider, K. Chudzikowski, Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks, Computers & Security 68 (2017) 145–159.

[63] Palo Alto Networks Inc., Cyberthreat report: Reconnaissance 2.0, https://www.paloaltonetworks.com/resources/whitepapers/cyber-threat-report-reconnaissance (Accessed 5 January 2019) (2018).

[64] T. R. Peltier, Information Security Policies, Procedures, and Standards: Guidelines for effective Information Security Management, Auerbach Publications, 2016.

[65] J. P. Bagian, J. Gosbee, C. Z. Lee, L. Williams, S. D. McKnight, D. M. Mannos, The veterans affairs root cause analysis system in action, The Joint Commission Journal on Quality Improvement 28 (10) (2002) 531–545.

[66] B. Andersen, T. Fagerhaug, Root cause analysis: simplified tools and techniques, ASQ Quality Press, 2006.

[67] I. Blickstein, M. Boito, J. A. Drezner, J. Dryden, K. Horn, J. G. Kallimani, M. C. Libicki, M. McKernan, R. C. Molander, C. Nemfakos, et al., Root Cause Analyses of Nunn-McCurdy Breaches, Volume 1, Rand Corporation, 2011.

[68] N. Ismail, Cyber security professionals blame ceos for data breaches, 24 July, http://www.information-age.com/cyber-security-professionals-blame-ceos-data-breaches-123467499/ (Accessed 5 January 2019) (2017).

[69] J. Keane, Pointing the finger of blame over a data breach, 23 June, http://www.idgconnect.com/abstract/10059/pointing-finger-blame-breach (Accessed 7 January 2019) (2015).

[70] A. Carman, OPM breach diverges into finger-pointing and dispute over initial detection, 15 June, https://www.scmagazine.com/opm-breach-detection-and-breadth-remains-murky/article/532308/ (Accessed 5 January 2019) (2015).

[71] D. L. Shinder, Pointing the digital finger: Who's really to blame for security breaches?, 24 May, https://techtalk.gfi.com/pointing-the-digital-finger-whos-really-to-blame-for-security-breaches/ (Accessed 5 January 2019) (2016).

[72] CIO Staff, Data on 26.5M Veterans Stolen from VA Staffer's Home, 22 May, https://www.cio.com/article/2446441/security-privacy/data-on-26-5m-veterans-stolen-from-va-staffer-s-home.html (Accessed 7 January 2019) (2006).

[73] BBC, TalkTalk fined £400,000 for theft of customer details, 05 October, http://www.bbc.co.uk/news/business-37565367 (Accessed 5 January 2019) (2016).

[74] M. Isaac, K. Benner, S. Frenkel, Uber hid 2016 breach, paying hackers to delete stolen data, 1 November, https://www.nytimes.com/2017/11/21/technology/uber-hack.html?_r=0 (Accessed 5 January 2019) (2017).

[75] Reuters, Austria's FACC, hit by cyber fraud, fires CEO, 25 May, https://www.reuters.com/article/us-facc-ceo/austrias-facc-hit-by-cyber-fraud-fires-ceo-idUSKCN0YG0ZF (Accessed 7 January 2019) (2016).

[76] J. Horowitz, D. Wiener-Bronner, Equifax's Chief Information Officer and Chief Security Officer are out, 15 September, http://money.cnn.com/2017/09/15/news/equifax-top-executives-retiring/index.html (Accessed 5 January 2019) (2017).

[77] J. Russell, Equifax CEO Richard Smith has 'retired' following huge data breach, https://techcrunch.com/2017/09/26/equifax-ceo-richard-smith-has-retired-following-huge-data-breach/ (Accessed 7 January 2019) (2017).

[78] Reuters, British Airways IT outage caused by contractor who switched off power, 2 June, https://www.cnbc.com/2017/06/02/british-airways-it-outage-caused-by-contractor-who-switched-off-power-times.html (Accessed 7 January 2019) (2017).

[79] K. Swisher, Yahoo's head lawyer is taking the fall for its hacking, while CEO Marissa Mayer is getting her pay docked, 1 March, https://www.recode.net/2017/3/1/14783686/yahoos-lawyer-ousted-hacking-marissa-mayer-pay-docked (Accessed 7 January 2019) (2017).

[80] M. Donnelly, Amy Pascal Says She Was 'Fired,' Talks Leaked Sony Emails and Angelina Jolie, 12 February, https://www.thewrap.com/amy-pascal-says-she-was-fired-talks-leaked-sony-emails-and-angelina-jolie/ (Accessed 5 January 2019) (2015).

[81] CIO Staff, VA Official Resigns Due to Data Theft, 31 May, https://www.cio.com/article/2446294/security-privacy/va-official-resigns-due-to-data-theft.html (Accessed 5 January 2019) (2006).

[82] K. Renaud, Clinical and Information Governance Proposes; Human Fallibility Disposes, Clinical Governance: An International Journal 19 (2) (2014) 94–109.

[83] C. Arthur, Cyber Wars, Kogan Page Ltd, 2018.

[84] M. Siponen, M. A. Mahmood, S. Pahnila, Employees' adherence to information security policies: An exploratory field study, Information & Management 51 (2) (2014) 217–224.

[85] S. W. Smith, Humans in the loop: Human-computer interaction and security, IEEE Security & Privacy 99 (3) (2003) 75–79.

[86] W. Hart, Verdraaide Organisaties, Kluwer, 2013.

[87] S. B. Lipner, The birth and death of the orange book, IEEE Annals of the History of Computing 37 (2) (2015) 19–31.

[88] M. Warner, Cybersecurity: a pre-history, Intelligence and National Security 27 (5) (2012) 781–799.

[89] L. A. Bebchuk, M. J. Roe, A theory of path dependence in corporate ownership and governance, Stan. L. Rev. 52 (1999) 127.

[90] L. Dobusch, J. Kapeller, Breaking new paths: Theory and method in path dependence research, Schmalenbach Business Review 65 (3) (2013) 288–311.

[91] G. Siboni, D. Siman-Tov, Cyberspace Extortion: North Korea versus the United States, December 23 INSS Insight No. 646 http://www.inss.org.il/publication/cyberspace-extortion-north-korea-versus-the-united-states/ (Accessed 7/1/2019) (2014).

[92] P. Bright, Sony hacked yet again, plaintext passwords, e-mails, DOB posted, 3 June, https://arstechnica.com/tech-policy/2011/06/sony-hacked-yet-again-plaintext-passwords-posted/ (Accessed 5 January 2019) (2011).

[93] P. Cooper, Cognitive Active Cyber Defense: Finding Value through Hacking Human Nature, Journal of Law & Cyber Warfare 5 (2) (2017) 57–172.

[94] C. Castelli, B. Gabriel, J. Yates, P. Booth, Strengthening digital society against cyber shocks — Key findings from The Global State of Information Security Survey 2018, https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey/strengthening-digital-society-against-cyber-shocks.html (Accessed 5 January 2019) (2018).

[95] M. T. Hopkins, The Exceptionalist's Approach to Private Sector Cybersecurity: A Marque and Reprisal Model, Ph.D. thesis, George Washington University Law School (2011).

[96] J. Bort, How The Hackers Broke Into Sony And Why It Could Happen To Any Company, 19 December, http://uk.businessinsider.com/how-the-hackers-broke-into-sony-2014-12?r=US&IR=T (Accessed 10 March 2018) (2014).

[97] A. Martin, LulzSec's Sony Hack Really Was as Simple as It Claimed, 22 September, https://www.theatlantic.com/technology/archive/2011/09/lulzsecs-sony-hack-really-was-simple-it-claimed/335527/ (Accessed 5 January 2019) (2011).

[98] T. Brewster, Revealed: Marriott's 500 Million Hack Came After A String Of Security Breaches, 3 December, https://www.forbes.com/sites/thomasbrewster/2018/12/03/revealed-marriotts-500-million-hack-came-after-a-string-of-security-breaches/ (Accessed 5 January 2019) (2018).

[99] World Economic Forum, The Global Risks Report 2017 12th Edition, http://www3.weforum.org/docs/GRR17_Report_web.pdf (Accessed 5 January 2019) (2017).

[100] H. Paz, F. Vega-Ramos, F. Arreola-Villa, Understanding hurricane resistance and resilience in tropical dry forest trees: A functional traits approach, Forest Ecology and Management 426 (2018) 115–122.

[101] C. Gardi, L. Montanarella, D. Arrouays, A. Bispo, P. Lemanceau, C. Jolivet, C. Mulder, L. Ranjard, J. Römbke, M. Rutgers, et al., Soil biodiversity monitoring in Europe: ongoing activities and challenges, European Journal of Soil Science 60 (5) (2009) 807–819.

[102] E. Hollnagel, D. Woods, N. Leveson, Resilience Engineering: Concepts and Precepts, Ashgate Publishing, 2006.

[103] H. C. Pham, D. D. Pham, L. Brennan, J. Richardson, Information Security and People: A Conundrum for Compliance, Australasian Journal of Information Systems 21 (2017) 1–16.

[104] P. Bourdieu, The left hand and the right hand of the state, interview with R.P. Droit and T. Ferenczi. In Acts of Resistance: Against the New Myths of Our Time. Cambridge: Polity Press. (1998).

[105] P. E. Spector, Perceived control by employees: A meta-analysis of studies concerning autonomy and participation at work, Human Relations 39 (11) (1986) 1005–1016.

[106] L. D. Marquet, Turn the Ship Around! A True Story of Turning Followers into Leaders, Gildan Media, LLC, 2013.

[107] H. W. Heinrich, Industrial Accident Prevention. A Scientific Approach., 4th Edition, New York & London: McGraw-Hill Book Company, Inc., 1959.

[108] E. Hollnagel, Safety-I and Safety-II: The Past and Future of Safety Management, Ashgate Publishing, Ltd., 2014.

[109] S. Dekker, The Field Guide to Understanding 'Human Error', Ashgate Publishing, Ltd., 2014.

[110] C. Perrow, Normal Accident at Three Mile Island, Society 18 (5) (1981) 17–26.

[111] S. Dekker, P. Cilliers, J.-H. Hofmeyr, The complexity of failure: Implications of complexity theory for safety investigations, Safety Science 49 (6) (2011) 939–945.

[112] G. I. Rochlin, T. R. La Porte, K. H. Roberts, The self-designing high-reliability organization: Aircraft carrier flight operations at sea, Naval War College Review 51 (3) (1998) 97.

[113] K. H. Roberts, New challenges in organizational research: high reliability organizations, Industrial Crisis Quarterly 3 (2) (1989) 111–125.

[114] K. H. Roberts, Some characteristics of one type of high reliability organization, Organization Science 1 (2) (1990) 160–176.

[115] S. Dekker, Safety Differently: Human Factors for a New Era, CRC Press, Boca Raton, 2014.

[116] S. Dekker, Just Culture: Balancing Safety and Accountability, Ashgate Publishing, Ltd., Florida, USA, 2012.

[117] K. E. Weick, K. M. Sutcliffe, D. Obstfeld, Organizing for high reliability: Processes of collective mindfulness, Crisis Management 3 (1) (2008) 31–66.

[118] R. M. Wachter, P. J. Pronovost, Balancing "no blame" with accountability in patient safety, The New England Journal of Medicine 361 (14) (2009) 1401–1406.

[119] D. Beaty, The Naked Pilot, Elsevier, Burlington, USA, 2010.

[120] S. Dekker, Employees: a problem to control or solution to harness, Professional Safety 58 (8) (2014) 32–36.

[121] J. Carroll, A. C. Edmondson, Leading organisational learning in health care, BMJ Quality & Safety 11 (1) (2002) 51–56.

[122] S. Brostoff, M. A. Sasse, Safe and sound: a safety-critical approach to security, in: Proceedings of the 2001 workshop on New security paradigms, ACM, 2001, pp. 41–50.

[123] S. L. Pfleeger, M. A. Sasse, A. Furnham, From weakest link to security hero: Transforming staff security behavior, Journal of Homeland Security and Emergency Management 11 (4) (2014) 489–510.

[124] R. L. Burkhead, A phenomenological study of information security incidents experienced by information security professionals providing corporate information security incident management, Ph.D. thesis, Capella University (2014).

[125] I. Kirlappos, A. Beautement, M. A. Sasse, 'Comply or Die' Is Dead: Long live security-aware principal agents, in: International Conference on Financial Cryptography and Data Security, Springer, 2013, pp. 70–82.

[126] S. Dekker, Just culture: Who gets to draw the line?, Cognition, Technology & Work 11 (3) (2009) 177–185.

[127] T. W. Van der Schaaf, D. A. Lucas, A. R. Hale, Near Miss Reporting as a Safety Tool, Butterworth-Heinemann, 2013.

[128] A. C. Edmondson, Learning from failure in health care: frequent opportunities, pervasive barriers, BMJ Quality & Safety 13 (suppl 2) (2004) ii3–ii9.

[129] P. Hudson, Applying the lessons of high risk industries to health care, BMJ Quality & Safety 12 (suppl 1) (2003) i7–i12.

[130] E. Hollnagel, Risk + Barriers = Safety?, Safety Science 46 (2) (2008) 221–229.

[131] P. M. Fitts, M. Viteles, N. Barr, D. Brimhall, G. Finch, E. Gardner, W. Grether, W. Kellum, S. Stevens, Human engineering for an effective air-navigation and traffic-control system, and appendixes 1 thru 3, Tech. rep., Ohio State University Research Foundation Columbus (1951).

[132] S. W. Dekker, D. D. Woods, MABA-MABA or abracadabra? Progress on human–automation co-ordination, Cognition, Technology & Work 4 (4) (2002) 240–244.

[133] N. B. Sarter, D. D. Woods, C. E. Billings, Automation Surprises, Handbook of Human Factors and Ergonomics 2 (1997) 1926–1943.

[134] C. H. Tinsley, R. L. Dillon, P. M. Madsen, How to avoid catastrophe, Harvard Business Review 89 (4) (2011) 90–97.

[135] S. Dekker, Why do things go right?, 28 September, http://www.safetydifferently.com/why-do-things-go-right/ (Accessed 5 January 2019) (2018).

[136] MITRE Corporation, MITRE True Story Series, https://www.mitre.org/work/cybersecurity.html (Accessed 5 January 2019) (2009).

[137] E. Hollnagel, RAG — The resilience analysis grid, Farnham, UK: Ashgate, 2011.

[138] A. Falk, M. Kosfeld, The hidden costs of control, American Economic Review 96 (5) (2006) 1611–1630.

[139] C. Nemeth, R. Wears, D. Woods, E. Hollnagel, R. Cook, Minding the gaps: Creating Resilience in Health Care, Agency for Healthcare Research and Quality (US), 2008.

[140] Infosec Institute, Top 7 security threats for employees, https://resources.infosecinstitute.com/category/enterprise/securityawareness/employee-security-threats/ (Accessed 5 January 2019) (nd).

[141] Redscan, Human behaviour: How to prevent employee actions compromising your cyber security, 16 August, https://www.redscan.com/news/human-behaviour-prevent-employee-actions-compromising-cyber-security/ (Accessed 5 January 2019) (2017).

[142] S. K. White, How your employees put your organization at risk, 28 May, https://www.cio.com/article/2927598/security0/how-your-employees-put-your-organization-at-risk.html MAY 28 (Accessed 7 January 2019) (2015).

[143] CeBit Australia, Why your employees are your biggest cybersecurity risk (and what to do about it), 13 February, http://blog.cebit.com.au/why-employees-are-your-biggest-cyber-security-risk (Accessed 7 January 2019) (2018).

[144] Cofense, Cofense PhishMe - Employee Conditioning for Resiliency against Phishing, https://cofense.com/product-services/phishme/ (2019).

[145] Gophish, Gophish - Open-Source Phishing Framework , https://getgophish.com/ (2017).

[146] SECUSO, TORPEDO Version 1.0.9, 26 September, https://addons.mozilla.org/de/firefox/addon/torpedo-browser/ (2018).

[147] SECUSO, PassSec+ Version 2.1, 6 June, https://addons.mozilla.org/de/firefox/addon/passsec/ (2018).

[148] B. Ur, F. Alfieri, M. Aung, L. Bauer, N. Christin, J. Colnago, L. F. Cranor, H. Dixon, P. Emami Naeini, H. Habib, N. Johnson, W. Melicher, Design and evaluation of a data-driven password meter, in: Proceedings of the CHI Conference on Human Factors in Computing Systems, ACM, 2017, pp. 3775–3786.

[149] P. A. Grassi, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr, J. P. Richer, N. B. Lefkovitz, J. M. Danker, Y.-Y. Choong, K. Greene, M. F. Theofanos, Digital identity guidelines: Authentication and lifecycle management, Tech. rep., NIST, NIST Special Publication 800-63B https://doi.org/10.6028/NIST.SP.800-63b (2017).

[150] K. Renaud, V. Zimmermann, Nudging folks towards stronger password choices: providing certainty is the key, Behavioural Public Policy (2018) 1–31.

[151] M. W. Firmin, K. M. Gilson, Mission statement analysis of CCCU member institutions, Christian Higher Education 9 (1) (2009) 60–70.

[152] C. Fitzgerald, J. A. Cunningham, Inside the university technology transfer office: mission statement analysis, The Journal of Technology Transfer 41 (5) (2016) 1235–1246.

[153] Australian Government, Australia's cyber security strategy, https://cybersecuritystrategy.homeaffairs.gov.au/sites/all/themes/cybersecurity/img/PMC-Cyber-Strategy.pdf (Accessed 5 January 2019) (2016).

[154] Public Safety Canada, National cyber security strategy, https://www.canada.ca/en/public-safety-canada/news/2018/06/national-cyber-security-strategy.html (Accessed 5 January 2019) (2018).

[155] HM Government, National cyber security strategy 2016-2021, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (Accessed 5 January 2019) (2016).

[156] US Government, NATIONAL CYBER STRATEGY of the United States of America, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (Accessed 5 January 2019) (2018).

[157] New Zealand Department of the Prime Minister and Cabinet, National cyber policy office proactive release, https://dpmc.govt.nz/publications/new-zealands-cyber-security-strategy (Accessed 5 January 2019) (2018).

[158] New Zealand Department of the Prime Minister and Cabinet, New zealand's cyber security strategy, https://dpmc.govt.nz/publications/new-zealands-cyber-security-strategy (Accessed 26 January 2019) (2016).

[159] Hack Story, Captain Zap, 21 March, https://hackstory.net/Captain_Zap (Accessed 5 January 2019) (2011).

[160] K. D. Mitnick, W. L. Simon, The art of deception: Controlling the human element of security, John Wiley & Sons, 2011.

[161] C. Davis, interview: raphael gray a.k.a. curador, https://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/curador.html (Accessed 7 January 2019) (2001).

[162] Out-Law.com, Hacker Gary McKinnon, www.out-law.com/page-7228 (Accessed 5 January 2019) (2006).

[163] J. Verini, The Great Cyberheist, 10 November, https://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html (Accessed 5 January 2019) (2010).

[164] K. Poulsen, Record 13-Year Sentence for Hacker Max Vision, 2 October, https://www.wired.com/2010/02/max-vision-sentencing/ (Accessed 5 January 2019) (2010).

[165] Hacking News, Testimony of a professional hacker – How Hackers Fool Your Employees, 24 May, http://www.hackingnews.com/hacking-groups/testimony-professional-hacker-fooled-employees-companies/ (Accessed 7 January 2019) (2015).

[166] USA, In The United States District Court For The Eastern District Of Virginia Alexandria Division. Criminal Case 1:16-cr-042, https://www.justice.gov/opa/file/896326/download (Accessed 5 January 2019) (2016).

Appendix A. Extracting Problems

Appendix A.1. ***Government-Identified Problems***

Methodology

Our analysis within the problematization approach was informed by the investigations into similar documents carried out by [151, 152]. The sentences were coded, in terms of whether they included or addressed:

(1) a mention of a specific problem in the cyber area,

(2) a new control or measure to be exerted as a response to a problem,

(3) a strategic aim, a statement of a specific allocation of funds or an aspirational dimension for improving cybersecurity indicating a current lack or insufficiency.

Using these categories helped us to derive the matching "problems" that the codes referred to. We pooled all problems across the different strategy documents, industry reports (Section Appendix A.2) and hacker statements (Section Appendix A.3), to arrive at a superset of problems as seen by the big players in cybersecurity today.

The problems derived in this and subsequent sections (Pi) refer to those listed in Table 1. Due to the post-analysis clustering of problems derived from different sources, they do not appear in sequential order in the text.

To analyse the government strategy documents, we scrutinised statements in the foreword and the executive summary, or introduction where these were not available. These parts of the document condense the purpose and the aspects that the writers consider most salient and necessary to communicate to citizens. By focusing on these sections, we can unravel the purposes of government, by reflecting on what they consider worthy of inclusion in the beginning of the policies i.e the most pressing problems that the strategy is aiming to address.

Australia [153]

The Hon Malcolm Turnbull MP launches the report by pointing towards the benefits of an open Internet. He then says that "*businesses need to ensure their cybersecurity practices are robust and up to date*" [p.2]. The "need to ensure" suggests that this might not be happening at present leading to **Problem P4:** Not following Security Best Practice. The Prime Minister returns to this theme on the next page by stating: "*better educate and empower our employees to use sound practices online [...] promote an improved institutional cyber culture and raise awareness of cyber practice across government and business to enable all Australians to be secure online*" [p.3]. From this, we derive **Problem P1:** Lack of Cyber Awareness, Knowledge and Skills.

The next paragraph refers to "*malicious actors—including serious and organised criminal syndicates and foreign adversaries*" and the fact that their methods are rapidly evolving, leading to **Problem P7:** Cyber Criminals. They also mention improving their capacity to tackle cyber crime [p.7] encapsulated in **Problem P10**: Cyber Criminal Detection & Prosecution.

He then refers to the risk of trusted insiders: "*the most damaging risk to government or business online security is not 'malware' but 'warmware'; the ability of a trusted insider to cause massive disruption to a network or to use legitimate access to obtain classified material and then illegally disclose it.*" [p.3]. This is summarised as **Problem P6:** Malicious Employees (i.e. the 'insider threat').

The Prime Minister states that he will "*appoint a Minister Assisting the Prime Minister on cybersecurity and a Special Adviser on cybersecurity in my Department*" [p.3]. This suggests that there has been a lack of leadership in government, which he plans to address. This is **Problem 14**: Lack of Leadership. They also state that: *"We will better detect, deter and respond to cyber security threats and better anticipate risks."* **Problem P13:** Inability to Defend/Respond.

"*The cybersecurity industry is in its relative infancy but undergoing rapid growth [...] We can use technology as a means to manage the threats and risks that come with being online and interconnected—and to grow our true potential*" [p.3]. The formulation hints at a current lack of innovative technology, leading to **Problem P11:** lack of local innovation in cybersecurity.

On page 3, the document states "*...promote international cyber cooperation*" hinting at a current lack thereof: **Problem P12:** Lack of Global Communication & Collaboration. Also, that *"It requires partnership involving governments, the private sector and the community"* suggests **Problem P5:** Not sharing Responsibility.

Page 8 mentions: *"With better focused cybersecurity research and development that responds to the needs of industry and governments"* [p.8]. The expressed need for researcher effort is formulated as (**Problem P16:** Lack of Targeted Research).

Finally, the summary mentions plans for developing more home-grown cyber skills, defensive capacity and security awareness "*all Australians understand the risks and benefits of the Internet and how to protect themselves online, through sustained joint public-private awareness initiatives and education campaigns*" [p.9]. This confirms P1.

Canada [154]

The Hon Ralph Goodale, Minister of Public Safety and Emergency Preparedness, says, on p.I: "*Major corporations, industries and our international allies and partners are engaged in the global cyber challenge. But many others are not — representing a significant risk*". Here he suggests that some people are not taking their responsibility for cybersecurity seriously enough (P5). There is also mention of *"low security awareness*" [p.2] (P1).

Later on the same page, he states "*an emphasis on the enormous potential of Canada's increased leadership in this field*". This suggests that leadership potential is there, but is not currently being realised (P14). Also, that there will be *"funding to foster innovation"*[p.III] (P11) and support for "*advanced research*" [p.3] (P16).

He concludes the foreword with a statement of three measures, each of which suggest a solution to a problem. The first is: "*Funding for the new Canadian Centre for cybersecurity to support leadership and collaboration between different levels of government and international partners [...]*" [p.II]. This confirms that a lack of leadership is considered to be a problem, but also that there is a lack of collaboration both within the Canadian government and internationally (P12 & P14). Moreover, he mentions that they plan better to *"respond to evolving threats, and defend critical government and private sector systems"* [p.3] (P13). There is also a sense that there is a need for trusted advice: *"while providing a clear and trusted resource for Canadian citizens and businesses"* [p.III] (**Problem P17:** Lack of Trusted Advice).

The second measure is: "*The creation of the National Cybercrime Coordination Unit to expand the RCMP's capacity to investigate cybercrime, establishing a coordination hub for both domestic and international partners.*" (P7, P10 & P12).

The third measure is: "*Funding to foster innovation and economic growth, and the development of Canadian cyber talent.*" which confirms P11 and indicates a need for skilled personnel adding **Problem P9:** Lack of Cybersecurity Professionals.

The UK [155]

The Rt Hon Philip Hammond MP, Chancellor of the Exchequer and The Rt Hon Ben Gummer MP, Minister for the Cabinet Office and Paymaster General introduce this strategy document. Here some of the previously-identified problems are confirmed. Stating that "*Cyber skills need to reach into every profession*" [p.6], also on pages 9 and 10, confirms P1. Also, the need for everyone to play their part is mentioned: *"Managing and mitigating those threats is a task for us all"* [p.7] (P5). "*Government has a clear leadership role, but we will also foster a wider commercial ecosystem, recognising where industry can innovate faster than us*" [p.6]. There is further mention on pages 9 and 10, confirming P11 & P14. The document also states that "*...there will always be attempts to exploit weaknesses to launch cyber attacks*" [p.9] repeating P7 & P10 and adding **Problem P8:** Software vulnerabilities. A lack of communication, collaboration and leadership is suggested in:"*We will also develop relationships with new partners to build their levels of cybersecurity and protect UK interests overseas*" and "*sharing knowledge, addressing systemic vulnerabilties and providing leadership on key national cybersecurity issues*" [p.9] (P12 & P14).

The statement "*We must therefore set ourselves the highest standards of cybersecurity and ensure we adhere to them*" [p.7], also on page 10, confirms P4 and adds **Problem P3:** Lack of Policies and Compliance.

The authors further state that"*...everyone has a part to play in our national response. It's why this strategy is an unprecedented exercise in transparency. We can no longer afford to have this discussion behind closed doors*" [p.6] (P12 & P14).

"*We detect, understand, investigate and disrupt hostile action taken against us, pursuing and prosecuting offenders. We have the means to take offensive action in cyberspace, should we choose to do so*" [p.9] (P10).

Next,"*This includes a drive to get the best young minds into cybersecurity*" [p.6] indicates a current lack of cyber security professionals (P9). Finally, the need for the ability to defend and respond is expressed in"*...we will ensure that the Armed Forces can assist in the event of a significant*

national cyber attack" [p.10] (P13).

The USA [156]

Again, some of the previous problems are referred to by President Donald Trump. He states that *"adversaries have increased the frequency and sophistication of their malicious cyber activities"* [p.I] (P7 & P10).

There is mention of the activities of hostile nation states [p.1] "Our competitors and adversaries [...] engaging in pernicious economic espionage and malicious cyber activities" [p.1] (**Problem P15:** Hostile Nations). Also on [p.2]: *...economic espionage and trillions of dollars of intellectual property theft. "We have required departments and agencies to remove software vulnerable to various security risks. We have taken action to hold department and agency heads accountable for managing cybersecurity risks to the systems they control, while empowering them to provide adequate security"*[p.I] This statement confirms P4 & P8 and adds **Problem P2**: Lack of Accountability. A lack of local innovation and research is implied by *"fostering strong domestic innovation"*[p.1]. (P11) and *"prioritize national research"*[p.9] (P16). The global aspect of cybersecurity and the role of leadership are mentioned in *"Expand American influence abroad"* [p.1] (P12) and *"We will continue to lead the world in securing a prosperous cyber future"* [p.2] (P14). The need for defence is expressed in *"have faced challenges [...] detecting, responding to, and recovering from incidents"* [p.2] (P13).

New Zealand [157, 158]

Hon Amy Adams, Minister for Communications, introduces this strategy document [157]. On page 2: "*The threat to New Zealanders, and the New Zealand economy from cyber intrusions*" and "*Perpetrators can range from a lone hacker through to organised criminal groups, activists or state-sponsored actors who operate domestically and internationally.*" (P7).

"*Only 65% of businesses are confident that their information technology security systems are effective*" [p.2]. (P8). "*it is vital we place a strong focus on securing our information systems and building the skills*" [p.2] (P8, P1)

On page 2:"*Improving our ability to handle cybercrime*" (P13) and "*engaging with other countries on cyber security issues and the international management of the Internet is also important*" (P12). "*looking for private sector support*" [p.2] (P5). "*Victims, including businesses, often do not report incidents to law enforcement or disclose them publicly*" (Introduces: **P18**: Victims not reporting cyber incidents).

On page 4, the document cites a number of insecure behaviours that users engage in, and on page 5: "*New Zealanders at all levels will have the skills and tools to protect themselves online*" evidencing P1. Also: "*... makes it hard to distinguish between the actions of state-sponsored cyber intruders, organised cyber-criminal groups or an isolated computer hacker*" (P10, P15) and "*the inevitable weaknesses or gaps in the protection of these information assets, and the existence of attackers who can exploit these vulnerabilities for their own advantage*" (P7, P8)

On page 5:"*Malicious cyber techniques can be deployed from any location*" (P10) "*Government agencies and businesses need to have timely, actionable cyber security information and advice and be able to deal with a trusted agency when they have a cyber security incident*" (P17) "*ensure preparedness for major cyber incidents*" (P13)

On page 6: "*New Zealand's cyber security expertise also needs to grow so that businesses and organisations can source the technical staff required to carry out ICT security.*" (P9) "*giving New Zealanders the tools to change their online behaviour. A joined-up approach will also be critical to*

provide an effective, customer-focused response to cybercrime." (P1, P13) "*International engagement is essential for cyber security.*" (P12)

In 2018, New Zealand published a document titled "National Cyber Policy Office Proactive Release", which refreshes their cyber security policy [158]. We thus problematized this document too. We will not repeat the previously-identified problems, only add any new ones that were introduced. The Hon Clare Curran, Minister of Broadcasting, Communications and Digital Media, introduces this strategy document.

On pages 2: *"system-wide leadership"* (P14). The statement *"provide cybersecurity advice and guidance to hundreds of organisations of national significance*" [p.2], also on page 7, confirms P17.

This policy acknowledges the fact that the cyber threat landscape is systemic: *"risks have effects across the system, beyond the remit of any single agency"* [p.7]. Also on page 7 (Introduces P2, confirms P5 & P12).

On page 9: *"investing in cyber security research"* (P16).

Appendix A.2. ***Industry-Identified Problems***

To reveal the cybersecurity threats and problems, as identified by industry, we examined security reports from global organisations.

Methodology

Similar to the previous analysis, to identify problems in cybersecurity from an industry perspective, we coded statements using the comprehensive list of problems (Tables 1 and 2), using the previously identified categories to support the identification process.

CheckPoint [52]

The Check Point 2018 Security Report analyses major security incidents caused by cyber criminals (P7) and trends across the cybersecurity landscape. It finds that 97% of organisations are using out-dated cybersecurity technologies and that as long as "*organisations remain uneducated about the necessity of maintaining their cybersecurity hygiene, we should not be surprised to see these evolving attacks continue in the years ahead*" [p.11]. Both indicate a lack of knowledge (P1) and a lack to follow security best practices (P4). Further, a "*lack of understanding regarding the responsibility*" [p.35] for, e.g., cloud services is identified as a problem (P2). The report also highlights the need for understanding the shared responsibility between customers and providers [p.7, p.23] (P5). They also find phishing that takes "*advantage of arguably the most vulnerable part of any network's security, the human element*" [p.33] to be one of the most common attacks. Also, an increase in the use of "*basic hacking techniques that rely on human error and social engineering*" [p.37] is suspected. It seems this does not only apply to end users but also 77% of IT professionals feel their security teams are unprepared for today's cybersecurity challenges indicating a general lack of awareness, knowledge and skills (P1). Suggested measures include training of employees (P1), following security best practices (P4) and having "*both the correct policies and technology*" [p.41] (P3, P8) in place.

Cisco [46]

The Cisco 2018 Annual cybersecurity Report describes the attack landscape that mainly includes cyber criminals (P7) as well as insider threats (P6), and the defender landscape with insights from more than 3600 respondents in 26 countries. It states that "*WannaCry and Nyetya could have been prevented, or their impact muted, if more organisations had applied basic security best*

practices such as patching vulnerabilities, establishing appropriate processes and policies for incident response" [p.7] which indicates a lack of following security best practices (P4), but also software vulnerabilities (P8) and a lack of policies (P3). The report further identifies a "*lack of clarity around who exactly is responsible*" [p.24] (P2) and a "*lack of trained personnel as an obstacle to enhancing security defenses in many organisations*" [p.10]. This refers to lack of cybersecurity professionals (P9) and at the same time a lack of knowledge and skills (P1) also described as "*security team skills gap"* [p.35]. The report suggests automation to overcome skills and resource gaps (P1), "user training and accountability" [p.21] (P1, P2), and the implementation of appropriate policies (P3).

Microsoft [53]

The Microsoft Security Intelligence Report sees social engineering, poorly secured cloud apps and legitimate software platform features as "*low hanging fruits*" [p.15] for cyber criminals (P7). Potential problems thus include unsuspecting and distracted users (P1) as well as a failure to follow security best practices such as encryption (P4). The misuse of legitimate software platform features can be classified as P8. The report suggests security awareness training (P1) and adopting security hygiene and best practices (P4).

Palo Alto [63]

The Palo Alto Networks Cyberthreat Report states that "*targeted attacks often start with the weakest links in organisations' defenses: their endpoints*" which is essentially the humans in the system (P1). It also finds that security best practices are often not extended to backup servers (P4) making them an easy target for cyber criminals (P7) and tools that "*discover new vulnerabilities*" [p.4] (P8). They suggest automating technology, limiting user access with appropriate policies (P3), monitoring user behaviour and implementing security measures such as multi-factor authentication to prevent security incidents confirming the above-mentioned problems.

Symantec [54]

The Symantec Internet Security Threat Report identifies spear-phishing emails as the most widely used infection vector and that "*often the person sitting behind a computer can be the weakest link in an organisation's security*" (P1). User training is suggested to minimise threats. The report also finds that users "*continue to make life easy*" [p.50] for "*greedy criminals*" [p.16] (P7) or malicious insiders (P6), e.g., by using older Android operating systems and thus not following security best practices (P4). However, also the technology itself by often not being powerful enough to run the latest version contributes to the problem (P8).

Appendix A.3. ***Hacker-Identified Problems***

Methodology

Similar to the previous analyses, to identify problems in cybersecurity from a hacker perspective, we coded published hacker statements using the comprehensive list of problems (Tables 1 and 2), to support the identification process.

Analysis

In 1981 a hacker called Captain Zap hacked into AT&T's computers [159]. In an interview he said that the big organisations who control information technologies " *are still causing the failure of the security of millions due to their greed and inability to allow others to see the magic behind the scenes*". This suggests that some pose monetary benefits above the responsibility for security

confirming P2. He also says: "*And then we have the lack of understanding from the users who will let you know anything that you need to know if you just call them and ask. An authoritarian voice with the right combination of buzz words and a bit of humor will get you past anyone on the phone.*" This confirms P1. Finally, he says: "*any form of so-called law enforcement is sadly lacking and grossly understaffed when it comes to computer related incidents*", confirming P10.

In 1995, the well known Hacker of Humans, Kevin Mitnick [160], was arrested. Having served his sentence, he now runs Mitnick Security Consulting. Mitnick said "*The key to social engineering is influencing a person to do something that allows the hacker to gain access to information or your network.*" confirming P1.

In 2000, a hacker called *curador* was charged for his cyber crimes. In an interview [161], he said: "*There are a lot of people out there who won't even safeguard their own safety, let alone the safety of their customers. At the end of the day, it's the fault of these companies. The buck does stop with them*". This confirms P2.

Gary McKinnon was arrested in 2006 for hacking into US military computers. He said: "*I used commercially-available off-the-shelf software, to scan military networks for blank passwords*" [162]. He exploited technical vulnerabilities, caused by the software installer not resetting the default password, and the software developer not forcing the change during installation. This confirms P4 & P8.

In 2010, a cyber criminal called Albert Gonzalez was arrested [163] for exploiting vulnerabilities in website software to steal credit card numbers. He said: "*I went to their Web Site, and I looked at their shopping-cart software, and within five minutes, I found a problem*". P8 is again confirmed. Max Butler, who also stole credit card details online, wrote a letter to the judge in his case [164], in which he talks about the need for his own high levels of technical expertise in helping the US government and the military to tighten up their network security. This again confirms P8.

In 2015, a professional hacker explained that they use emails to entice employees to click on links [165]. The hacker uses information posted on social networks to help compose emails that are likely to succeed in enticing the employee. This confirms P1. The hacker also makes use of keylogging software, which could be installed via a phishing email, or via a device plugged into the oblivious victim's computer. This confirms P1 & P8.

In 2016, the Court Records in the case against Ardit Ferizi reports that the hacker compromised a web server, probably using a SQL injection attack, and was able to steal thousands of personal records belonging to a company's customers [166]. He took advantage of software vulnerabilities to breach the system, confirming P8.