Information Systems Frontiers
https://doi.org/10.1007/s10796-024-10511-z

When Your Thing Won't Behave: Security Governance in the Internet of Things

Martin Brennecke[1] · Gilbert Fridgen[1] · Jan Jöhnk[2] · Sven Radszuwill[2] · Johannes Sedlmeir[1]

Accepted: 30 June 2024

Abstract
In the Internet of Things (IoT), interconnected smart things enable new products and services in cyber-physical systems. Yet, smart things not only inherit information technology (IT) security risks from their digital components, but they may also aggravate them through the use of technology platforms (TPs). In the context of the IoT, TPs describe a tangible (e.g., hardware) or intangible (e.g., software and standards) general-purpose technology that is shared between different models of smart things. While TPs are evolving rapidly owing to their functional and economic benefits, this is partly to the detriment of security, as several recent IoT security incidents demonstrate. We address this problem by formalizing the situation's dynamics with an established risk quantification approach from platforms in the automotive industry, namely a Bernoulli mixture model. We outline and discuss the implications of relevant parameters for security risks of TP use in the IoT, i.e., correlation and heterogeneity, vulnerability probability and conformity costs, exploit probability and non-conformity costs, as well as TP connectivity. We argue that these parameters should be considered in IoT governance decisions and delineate prescriptive governance implications, identifying potential counter-measures at the individual, organizational, and regulatory levels.

Keywords Information Security · Internet of Things (IoT) · IT Governance · IT Security · Risk Analysis · Security Breach

Managerial Relevance Statement

This paper provides prescriptive governance implications to cope with Internet of Things (IoT) security risks resulting from the use of technology platforms (TPs). In simple terms, we argue that while allowing for several different TPs increases the risk of a security incident, large-scale exploits are more likely for homogeneous TP use. Further, considering the correlation between TPs is important because diversification-related security governance measures may be less effective if two TPs' vulnerabilities are highly correlated. Finally, as we currently observe in practice, an increasing number of connected smart things makes IoT security across TPs particularly prone to large-scale exploits. Our governance implications address individuals (i.e., professional or private end-users) using smart things, manufacturers that build and distribute such smart things, and suppliers of TPs as critical component across different models of smart things. We further consider policymakers, regulators, and authorities that provide the guardrails for smart thing adoption and risk management. Summarizing, we provide practitioners with a better understanding of why and how TPs pose security risks to smart thing adoption in the IoT, help quantify and assess the associated risks, and stimulate discussions on appropriate measures to mitigate these risks.

✉ Jan Jöhnk
jan.joehnk@fim-rc.de

Martin Brennecke
martin.brennecke@uni.lu

Gilbert Fridgen
gilbert.fridgen@uni.lu

Sven Radszuwill
sven@radszuwill.de

Johannes Sedlmeir
johannes.sedlmeir@uni.lu

[1] Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, 29 Av. J.F. Kennedy, Luxembourg L-1855, Luxembourg

[2] FIM Research Institute for Information Management, University of Bayreuth, Universitätsstraße 30, Bayreuth D-95447, Germany

1 Introduction

"The spirits that I called" – In Disney's 1940 classic Fantasia, a sorcerer's apprentice is struggling with the acquired

Published online: 22 August 2024

power over a broom and its growing autonomy. Similar to the broom, webcams and other so-called smart things (Alter, 2019; Huber et al., 2024) were responsible for the worldwide distributed denial of service (DDoS) attack Mirai in 2016, executed by a botnet of more than 500,000 Internet of Things (IoT) devices and blocking the accessibility of popular web services such as AirBnB, Twitter, and Netflix (Dailymail, 2016; Walters & Jordan, 2016). Another example of the numerous recent security incidents is the ZigBee exploit, which could brick Philips Hue devices or use them for further DDoS attacks (Ronen et al., 2016). This exploit was able to spread to similar nearby devices via built-in wireless connectivity, causing cascade effects (Ronen et al., 2016). Further, the exploits Spectre and Meltdown used speculative execution in Intel, AMD, and ARM processors, potentially disclosing sensitive information on more than a billion devices (Kocher et al., 2018; Lipp et al., 2018). Also modern cars and their so-called controller area network (CAN) bus have also been prone to vulnerabilities (ICS-CERT., 2018a, b). This serial bus enables attackers to control safety-critical functionalities (e.g., braking) after gaining access via modern media and navigation systems or maintenance ports. Incidents like these have caused stricter regulatory demands on cybersecurity in general and of increasingly software-defined and autonomous vehicles in particular (ISO/SAE 21434:2021., 2021; Regulation EU 2018/858., 2018; Regulation EU 2019/2144., 2019). More recently, we further observed a backdoor in XZ Utils on Linux that was coincidentally caught in time before it could be exploited on a large scale (Lins et al., 2024), as well as the CrowdStrike Falcon update (CrowdStrike, 2024) on Microsoft Windows that impacted a wide variety of critical infrastructures and sectors, including but not limited to the financial services, health, and aviation industries (Financial Times, 2024).

All these incidents also exhibit at least three commonalities: They are associated with smart things and IoT, they use built-in networking features to spread rapidly, and they exploit a technology platform (TP) that is used in many different devices. Thus, guidance for IoT TP governance is needed; otherwise, security incidents will likely threaten the value capture driven by the opportunities of IoT, thereby transforming this paradigm into a costly *botnet of things*. The IoT paradigm describes an increasing number of smart things, which enable new interaction types for individuals, machines, and companies (Borgia, 2014; Ransbotham et al., 2016; Hartwich et al., 2023). Devices like webcams, refrigerators, microwaves, and even toothbrushes have become part of the IoT as simple embedded systems with access to the Internet (Neville-Neil, 2017), though they may not yet be actually smart (Huber et al., 2024). This drive to connect things to the Internet naturally increases the number of connections between objects in the physical realm (Aftergood, 2018; Li et al., 2015). Smart things in the IoT are equipped with high levels of connectivity on multiple layers (Whitmore et al., 2015). Intra-network connectivity refers to connectivity within companies or households (e.g., inside the (HAN)), typically providing value to the network's owner. For instance, household appliances (e.g., a refrigerator and a washing machine) can synchronize their energy consumption in a household to limit expensive peak loads (Waldo, 2002; Rieger et al., 2016). On the other hand, inter-network connectivity, i.e., interactions between smart things across companies or individual homes that form digital value networks, is typically based on communication over the Internet. Thus, a washing machine and solar cells of two different households could synchronize energy supply and energy demand via smart grids. In the course of the ongoing digital transformation, the number of physical objects equipped with sensors or communication and network interfaces and the number of smart things are growing, with new communication methods being created, and intra-network as well as inter-network connectivity increasing (Püschel et al., 2016; Yoo, 2010).

Security risks in the IoT strongly relate to smart things' quality and their underlying TPs. In contrast to considering a single entity, securing TPs in the IoT bears the risk of vulnerabilities shared across the platform with the potential to reinforce security incidents via the connectivity between many devices. Slaughter et al. (1998) differentiate between software quality costs for conformity, i.e., expenditures associated with the identification and prevention of defects that include corresponding opportunity costs (e.g., owing to longer development times), and costs of non-conformity, i.e., expenditures for rework, maintenance, liability damages, or litigation. We extend this distinction to TPs in IoT since the costs of conformity (e.g., during the TP design and the development of smart things) and non-conformity (e.g., in the event of an exploit owing to a platform vulnerability) equally apply to standardization, homogeneity, and "smartification" in IoT TPs. Thus, there is a trade-off between conformity costs and non-conformity costs considering the associated risks of corresponding TPs.

This trade-off raises questions concerning adequate individual, organizational, and regulatory reactions, i.e., which countermeasures should be taken to prevent or at least mitigate the effects of security incidents in the IoT. We see a need for effective management and governance procedures to balance the trade-off between conformity costs and non-conformity costs. In particular, the management and governance issues connected to TPs in the IoT must be considered from an individual's perspective (Almeida et al., 2015) as well as from the perspective of companies and regulators (Weber, 2010; Vermesan & Friess, 2022). Such a holistic approach is necessary to account for the high degree of interconnectivity and the blurring boundaries between actors in the IoT. These questions strongly relate to the standardization of IoT platforms and their governance.

Management and information systems (IS) research as well as policy-makers are paying increasing attention to (technology) platforms, including related governance questions and tensions (Thomas et al., 2014; Weigl et al., 2023). Particularly in the field of IS, researchers have previously investigated platform- and IoT-related challenges at the individual or behavioral level, at the organizational level, and at the regulatory or societal level. Based on this research – and at the intersection with emerging technologies – researchers also developed numerous alert systems and frameworks to address related challenges (Syed, 2020; Biswas et al., 2022, 2023).

At the same time, and along similar lines, the European Union (EU has started addressing cybersecurity challenges posed by the IoT, e.g., via the revision of the Product Liability Directive (COM/2022/495 final, 2022) and the Cyber Resilience Act (COM/2022/454 final., 2022). These measures are likely to substantially increase security requirements for products with digital components, including smart devices. Despite the recent ubiquity of challenges and risks related to TPs and IoT, the implications of TP use in the IoT and its impacts on information technology (IT) governance remain unexplored (Weber, 2013; Mohamad Noor & Haslina Hassan, 2019). Thus, like the sorcerer's apprentice, individuals, companies, and regulators are still struggling to achieve sufficient security governance in the IoT. Against this backdrop, we ask the following research question:

What are the implications of technology platform in the IoT for security governance at the individual, company, and regulatory levels?

We follow the research cycle proposed by Meredith et al. (1989) to address this question. "[A]ll research investigations involve a continuous, repetitive cycle of description, explanation, and testing" (cf. Meredith et al., 1989, p. 301). First, we seek to contribute to the descriptive body of knowledge by describing TP use in the IoT as well as its associated risks (Section 2). Second, we adopt a risk quantification approach developed for the automotive industry (Kang et al., 2015) to shed light on risk-related dynamics by addressing "the underlying causal structure of the theory" (cf. Meredith et al., 1989, p. 303), i.e., the antecedents, interdependencies, and implications of TP use in the IoT (Section 3). We demonstrate how the use of platforms and their risk quantification can be transferred to TPs in the IoT, using the case of BusyBox (ICS-CERT., 2022) as an illustrative example of a software suite that is used across millions of IoT devices – from (PLCs) to remote terminal units (RTUs) – and where risks have materialized, as highlighted by vulnerabilities related to its dynamic host configuration protocol (DHCP) clients (CVE-2016-2148., 2016), heap buffers (CVE-2018-1000517., 2018), and code execution (CVE-2022-48174., 2022). Third, we delineate prescriptive governance implications resulting from the inherent risks of TPs in the IoT (Section 4). In doing so, we seek to develop guidance to deal with an urgent real-world problem. We discuss the limitations of our research and conclude in Section 5.

2 Technology Platforms and Platform Security Risks in the IoT

2.1 Technology Platforms in the IoT

Platforms are considered an important paradigm for product management, new product development, as well as innovation and technological strategy (Facin et al., 2016). The concept of a platform comprises a set of different interpretations (Thomas et al., 2014). The literature either regards platforms from a technological perspective (Porch et al., 2015), with examples including IT platforms (Fichman, 2014), or as two-sided markets from a primarily economic perspective (Dibia & Wagner, 2015; Gawer, 2014). We follow the perspective of Fichman (2014), who define an IT platform as "a general-purpose technology that enables a family of applications and related business opportunities" (cf. Fichman, 2014, p. 132). In the IoT, such TPs can take different forms (Arnold et al., 2022). One may think of software platforms as operating systems or hardware platforms as processor families. Also, a TP is not necessarily tangible, but can also "be a set of standards" (cf. Gepp et al., 2016, p. 2). For instance, standards such as programming languages, protocols, or security guidelines can also represent TPs.

Regardless of whether they are tangible or intangible, TPs are typically used to achieve economies of scale via cost reductions over a set of components (Baldwin & Woodard, 2008). As the marginal costs of software are considered to be close to zero from a seller's perspective, the re-use of software components wherever possible is a logical consequence. Further, standards and standardized components enable cooperation in networks, because "firms with similar technological capabilities are likely to form strategic alliances and interact in a cooperative and competitive manner" (cf. hyu Kim et al., 2017, p. 2). In the automotive industry, efficient production is now inconceivable without platforms such as Volkswagen's modular transverse toolkit (Kang et al., 2015). With the rapidly increasing number of manufactured and deployed IoT devices, TPs receive growing relevance in the IoT. Indeed, the IoT sector is experiencing a development towards TP use, such as in the increasingly sensor- and software-defined automotive industry.

2.2 Technology Platform-related Risks, Vulnerabilities, and Exploits

We draw on Kang et al. (2015) for the concept of TP risk, the associated terms, the necessary adaptations to the specifics

of TPs in the IoT, as well as the differentiation between them. Kang et al. (2015) differentiate between *platforms, models, units, defects,* and *failures*. They define a *platform* as "a set of design components (i.e., software modules or physical parts) that are commonly shared by a range of different products" (Kang et al., 2015, p. 372and 37), using Toyota as an application example. The products under consideration are the brakes based on the same platform, i.e., an identical underlying design. A *model* describes an individual use case that is based on the common platform. In the Toyota case, the brake platform models correspond to the different car models, since each car model comes with its specific brake system that is based on the platform but adjusted to the specific car model. *Units* are entities of an instance of a model, e.g., the brake system in one manufactured Toyota Corolla.

To model TP risk, Kang et al. (2015) further introduce the notion of defect and failure. They define a design *defect* as a "design flaw that can potentially cause a failure in the course of a product's use" (cf. Kang et al., 2015, p. 373). Importantly, this is not to be confused with a unit's failure caused by a defectively manufactured product (Kang et al., 2015). For instance, the reliance of a Boeing 737 Max on a single sensor for its Maneuvering Characteristics Augmentation System (MCAS) can be considered a defect, whereas accidents caused by a malfunction of the sensor would represent a failure (Travis, 2019). This definition already implies that a *failure* refers to the manifestation of a defect. Failures can thus be modeled as random events, with the underlying probability distribution described by defects (Kang et al., 2015).

Notably, security risks in the IoT can further materialize not solely in relation to the hardware but also in the software being used. The resulting software security risks may not always be caused by the TP provider but can also be caused by third-party libraries the TP provider uses or adapts. One example of an IoT risk that materialized came in the form of three Apache *log4j* vulnerabilities, namely CVE-2021-44228, CVE-2021-45046, and CVE-2021-44832 (Microsoft Threat Intelligence., 2021). As log4j is a frequently used logging library, it affected a significant share of Java libraries used in both commercial and non-commercial settings. Consequently, many IoT TPs that comprise Java-based components, likely underlying billions (often interconnected) of smart devices, were affected. According to Microsoft, "the vulnerabilities presented a new attack vector and gained broad attention due to its severity and potential for widespread exploitation" (Microsoft Threat Intelligence., 2021). The Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly, at the time, further published a statement indicating that "this vulnerability poses a severe risk" (CISA., 2021). Similar risks can materialize in other digital infrastructures, including security and communication protocols.

We transfer these concepts to the specifics of TPs underlying IoT devices to model the risk of large-scale exploits – as for our application example, BusyBox. The Unix-based BusyBox is an open-source toolkit designed for mobile and embedded systems, as often found in IoT applications (ICS-CERT., 2022). The toolkit is widely used in products such as webcams (e.g., the D-Link Wi-Fi camera), routers and modems (e.g., AVM-Fritz!Box, Belkin, Linksys, and NetGear), smartphones (e.g., Nokia N900), television receivers (e.g., Dreambox), navigation systems (e.g., TomTom GO), and drones (e.g., AR Drone 2.0) (ICS-CERT., 2022; Arentz, 2005; TomTom, 2005; Labs, 2016). We use it as illustrative example for the definitions of the aforementioned concepts.

We apply Kang et al.'s (2015) definition of platforms to TPs in IoT, defining an *IoT platform* as any component type (hardware, software, or standard) that is shared between smart things. We regard a smart thing as a product – a "previously non-digital physical artifact" (cf. Yoo et al., 2012, p. 1399) that has been equipped with digital technology (Yoo et al., 2012). In our illustrative example, BusyBox represents the platform. Further, we consider an *IoT model* to be a type of smart thing that is based on a specific TP. This intails that different IoT models' physical shapes can vary substantially, as illustrated by the various models based on BusyBox, for instance, a Parrot AR Drone 2.0 and a D-Link web camera. The concept of an *IoT unit* is straightforward; we regard one physical, manufactured instance of a smart thing as one IoT unit.

While we also adopt the underlying definitions of *defect* and *failure* from Kang et al. (2015), their application and implications differ substantially between the automotive industry and the IoT field. Thus, following a classification by Howard & Longstaff (1998), we use the terms of *vulnerability* and *exploit* instead to account for additional, information systems-related specifics. A *vulnerability* is "a weakness [in the design, implementation, or configuration] of a system allowing unauthorized action" (cf. Howard & Longstaff, 1998, p. 14). This understanding is in line with other definitions that consider the concept of *vulnerability* to be directly related to the upper-level concept of *thing* (Syed, 2020). An *exploit*, on the other hand, represents a successful "group of attacks that can be distinguished from other attacks because of the distinctiveness of the attackers, attacks, objectives, sites, and timing" (cf. Howard & Longstaff, 1998, p. 15). An attack is specified by corresponding vulnerabilities, tools, actions, targets, and unauthorized results (Howard & Longstaff, 1998). Analogous to Kang et al.'s (2015) definition of a defect, a *vulnerability* refers to a flawed design, for instance, the possibility for malicious code injection in BusyBox via the *netstat* tool (Cybersecurityhelp., 2022). Thus, an *exploit* constitutes a manifestation of a vulnerability of the IoT platform, e.g., a successfully planted backdoor in

a D-Link DCS-930L webcam utilizing the vulnerability of BusyBox.

2.3 Platform Security Risks

In the context of IoT TPs, we understand *security* as an extension of the common *CIA triad* (confidentiality, integrity, and availability) that also considers access level and functional level security requirements (Meneghello et al., 2019). This interpretation demands control both over information processed by an individual smart thing as well as the impact of such processing on other components (e.g., individuals or other devices). In line with this understanding, platform security is concerned with "tangible and intangible assets relating to the wellbeing of either the individual or society at large" (cf. von Solms & van Niekerk, 2013, p. 101). Following von Solms & van Niekerk's (2013) definition of cybersecurity, we further include the entirety of all IoT devices in this assessment and do not solely refer to an individual's information and communication using a specific IoT device as the asset at risk.

Exploits such as the Mirai IoT botnet, which was based on the BusyBox TP vulnerability, illustrate that security breaches may not only affect a single smart thing according to the CIA triad, but rather risk the overall wellbeing of other smart things built on other TPs owing to DDoS attacks. As such, we argue that this holistic perspective is necessary. The overall security goals of the CIA triad (confidentiality, integrity, and availability) and its extensions (accountability, authenticity, non-repudiation, and reliability) remain unchanged in this interpretation in the context of the IoT (von Solms & van Niekerk, 2013; Siponen & Oinas-Kukkonen, 2007). Yet, considering the connectivity of smart things in the IoT, related work suggests increasing resilience to attacks as an additional cybersecurity goal, i.e., "[avoiding] single points of failure and [adjusting] to node failures" (Faber & Günther 2007, p. 3) .

Rainer Jr et al. (1991, p. 130) define *risk* as the condition "when an asset is vulnerable to a threat" and distinguish between *physical* threats (e.g., weather or fire) and *unauthorized or authorized access* as major threats to IT. Although unauthorized access is the most obvious security threat, authorized access can even be more influential because the access usually goes unnoticed. Further, Rainer Jr et al. (1991) note that threats can originate from *internal or external sources*. Security risks may occur at various levels, i.e., the application level, the organizational level, and the inter-organizational level (Bandyopadhyay et al., 1999). Applied to the IoT, these definitions and distinctions remain valid, but the characteristics of the IoT imply potential risks at all three levels owing to its physical components, human-machine interaction, and cross-organizational interactions (Sadeghi et al., 2015).

The IoT not only inherits classic IT security risks but also creates new security risks due to IoT-specific features (Zhou et al., 2019). According to Atzori et al. (2010), three IoT-specific vulnerabilities increase security risks for smart things: *Unattended components* that facilitate physical attacks, *accessibility* via wireless communication, and *reduced security measures* owing to limited energy and computing resources. We argue that the use of TPs in the IoT amplifies these vulnerabilities for two reasons. First, smart things built on a common TP are characterized by shared technical components as well as increased intra-network and inter-network connectivity in the IoT. Thus, although "platform sharing is considered an effective means of cost saving [...] it also runs the risk of propagating a particular failure" (Kang et al., 2015, p. 372) among smart things building on the same TP. This can lead to cascading effects even if only a single component is exploited. Second, although smart things share a common TP, they can still have distinct features that may prohibit or impede a simple platform-wide rollout of security countermeasures (e.g., patches). Thus, the degree of connectivity and the extent of variations across models may contribute to the risk of cascading TP-specific vulnerabilities. As a result, smart things in the IoT are attractive targets owing to their vulnerabilities and their frequent uses in critical infrastructures such as the internet of medical things (IoMT) (Wang et al., 2022) or environments of sensitive information such as the industrial IoT (IIoT) (Sadeghi et al., 2015; Eden et al., 2017; Miller & Rowe, 2012). We consider an IoT-specific analysis of platform security risks and the implications for appropriate governance measures to be a valuable addition to the existing body of knowledge.

In light of the aforementioned definitions and examples, the specific risk of a TP in the IoT can be summarized as follows: Owing to the sharing of identical technological components across a platform, a vulnerability's effect (i.e., the overall number of exploited units) can be substantial. Vulnerabilities of one smart thing model are likely to occur in a similar way (if not identically) in many other smart thing models that share the same TP. This is crucial because the key to successful platform strategies is to attract third-party vendors developing applications on the platform (Kim & Altmann, 2020). In this context, it does not matter if hardware, software, or a standard constitutes the TP. We want to point out that there are also other models for quantifying the risk or impact of IT security incidents, e.g. the IoT MicroMort model (Radanliev et al., 2018). In contrast, our focus lies on the risk of exploits of vulnerabilities that are correlated through the joint use of an IoT-specific TPs and an assessment of corresponding, potentially widespread, implications for security and resilience. Therefore, we will now elaborate on the modeling of such risks in TPs, based on the concepts of vulnerabilities and exploits.

3 Modeling Technology Platform Risks in the IoT

To model TP risk in the IoT, we use a Bernoulli mixture model, an established approach to model credit default risk in the financial sector (Bluhm et al., 2010; Giesecke, 2004; Giesecke & Weber, 2004). To outline the specifics of IoT TPs, we follow the modeling procedure of Kang et al. (2015) and transfer it to IoT TPs. To understand the modeling procedure, it is important to distinguish between the *ex-ante* and *ex-post* probability (or density) of an incident, i.e., respectively, before any observation and after having observed a certain event (Rausand et al., 2020) – in our case, an exploit. Platforms are usually designed with care, and a platform provider can be assumed to not purposefully design a vulnerable platform. However, vulnerabilities empirically cannot be avoided entirely. Further, some security issues only emerge with new technological developments. For instance, certain cryptographic libraries can become insecure because an attacker's computational power can increase or an attacker may get access to a capable quantum computer (Bhat & Giri, 2021). Thus, a vulnerability often only becomes apparent ex-post. For instance, when the BusyBox TP was first designed in 1995, the currently prevailing security incidents were not foreseeable, partly owing to the lack of technical possibilities at that time as well as the later arising use of the IoT. Thus, ex-ante, a platform design may be assumed to be free of vulnerabilities, yet after having observed exploits, ex-post, vulnerabilities become apparent.

We will now transfer Kang et al.'s (2015) model to TP in the IoT and contribute to the descriptive body of knowledge by describing TP use in the IoT as well as the associated security risks. Also, we derive governance implications for TPs in the IoT from this model. To not exceed this paper's scope, we refer to Bluhm et al. (2010) for a more detailed overview of Bernoulli mixture models. We use the notations in Table 1 to describe the mathematical model.

We inherit the following assumptions from Kang et al. (2015): Let $I_{i,k}$ denote the random variable representing whether or not unit k among model i is exploited, where $i \in \{1, \ldots, r\}$ and $k \in \{1, \ldots, N_i\}$. Let Θ_i denote the random variable representing the exploit probability for model i. Then:

Table 1 Mathematical Notations to Model TP Risks in the IoT

Notation	Description
r	Number of models based on the TP
$i \in \{1, ..., r\}$	Index of a model within the TP
m_i	Model i
N_i	Total number of deployed units of model i
p_g	Vulnerability probability of the TP
g_i	Exploit probability for model i
$\rho_{i,j}$	Correlation coefficient between model i and j
Y_i	Number of exploited units for model i
$X = \sum_{i=1}^{r} Y_i$	Number of exploited units for entire TP

A0: For each pair of units k_1 in model i_1 and k_2 in model i_2, the random variables I_{i_1,k_1} and I_{i_2,k_2} are independent and follow Bernoulli(Θ_{i_1}) and Bernoulli(Θ_{i_2}), respectively, for both $i_1 = i_2$ and $i_1 \neq i_2$ (*conditional independence*).

A1: $P(\Theta_{i_1} = g_{i_1}, \Theta_{i_2} = g_{i_2} \vee \Theta_{i_1} = 0, \Theta_{i_2} = 0) = 1$ (*perfect correlation*).

A2: Θ_{i_1} and Θ_{i_2} independently take one of two values, g_i and 0 (*independence*).

Our model can be thought of as describing two sequential incidents. Initially, to obtain a nonzero probability of exploited units of any model, a TP must contain a vulnerability. Subsequently, given that the TP is vulnerable, a specific exploit for this vulnerability is possible for each model m_i based on the TP. Thus, a TP has a vulnerability probability p_g, and each model m_i has an exploit probability g_i. Again, in case a vulnerability would have been known ex-ante, the platform would have been designed differently. In our view, any IT-related TP has a vulnerability probability $p_g > 0$ because perfect security by design is virtually impossible, as steady reports on the most recent IT security incidents emphasize. This is due to the heavy use of IT components, their fairly short lifecycles, complex system environments, and economic incentives for attackers, to name just a few reasons (Nicolescu et al., 2018). Further, exploits in most cases require a conscious action, implying knowledge of the vulnerability and the development of a suitable counterattack. Both require time and effort. Thus, a perfect TP security level is hard to achieve, and $p_g > 0$. On the other hand, most vulnerabilities can be fixed and are fixed after exploits emerge or responsible disclosure occurs (Arora et al., 2010), i.e., before a large number of units are exploited. Thus, in our view, the exploit probability can generally be assumed to be small.

Vulnerabilities that become public and remain unfixed for a long time are prone to exploits. In such cases, TPs in the IoT bear the subsequent risk of cascading an exploit through the network that connects individual devices. Thus, the risk of an exploit caused by a vulnerable TP can be amplified owing to the units' connectivity. A key question is whether the contagion becomes an epidemic and spreads rapidly, or whether it dies out. The threshold between these two cases is called the *epidemic threshold* (Prakash et al., 2012). There is evidence that the epidemic threshold can be very low for homogeneous networks (Prakash et al., 2012). On the other hand, connectivity also provides the possibility to rapidly spread countermeasures, even before cascade effects occur. The explicit modeling of such cascades (with both positive

and negative effects) has been the subject of research in other disciplines (Buldyrev et al., 2010; Watts, 2002; Helbing, 2013), and should also be subject to future research in the IoT. Although we do not look into cascade effects in particular, we connect our findings to the notion of cascade effects. For single units of each model, we distinguish the two states *exploit* and *no exploit*, which can be modeled as a Bernoulli trial (Kang et al., 2015). Thus, the exploit of a single unit is a random event occurring with probability g_i for model i of the TP, given the vulnerability in the TP. For instance, consider the aforementioned BusyBox as TP. Model m_1 could then denote the D-Link DCS-930L Home Network Webcam, model m_2 the D-Link DCS-932L Home Network Webcam, and model m_3 the TomTom GO 4 navigation system, since they all are based on BusyBox. The exploit probability g_i can vary for different models of the same platform, i.e., it may be more likely for model m_1 (D-Link DCS-930L webcam) to be exploited than for model m_2 (D-Link DCS-932L webcam), or for model m_3 (TomTom GO 4). With this denomination, a risk measure for exploits of a TP is given by the tail probability $P(X > \overline{x})$ (see Fig. 1), where $X = \sum_{i=1}^{r} Y_i$, and $\overline{x}$ is an arbitrary threshold that determines a large-scale exploit (Kang et al., 2015; Fabozzi et al., 2007; Roy, 1952). In other words, $P(X > \overline{x})$ denotes the probability that more than $\overline{x}$ units across all models of a TP in the IoT are exploited. Although we do not focus on cascade effects in this paper, considering $\overline{x}$ as the epidemic threshold is intriguing. Since more than $\overline{x}$ exploited units will possibly lead to subsequent cascade effects that spread through the network, this strongly amplifies an exploit's impacts. For instance, 3,000 D-Link DCS-930L webcams, 2, 000 D-Link DCS-932L, and 5, 000 TomTom GO 4 navigation systems exploited add up to 10,000 exploited units of the BusyBox TP. If $\overline{x} = 9,000$, the epidemic threshold would have been surpassed, and cascade effects likely propagate the exploit throughout the network. A low probability of facing many exploited units is desirable for all involved parties, i.e., the TP supplier (e.g., BusyBox's developers), manufacturers using the TP (e.g., D-Link and TomTom), individuals using the corresponding smart thing, as well as regulators. Figure 1 illustrates the denominations.

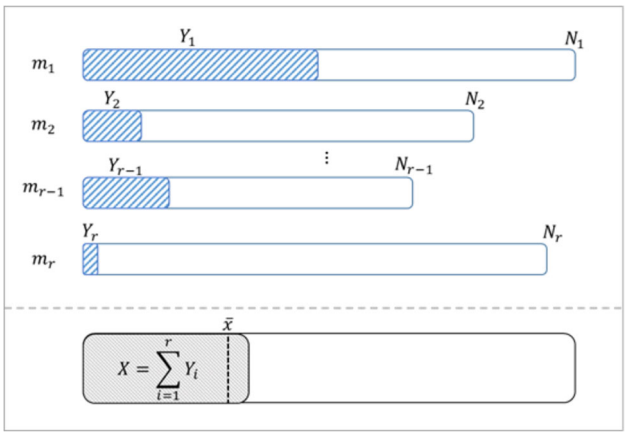

Fig. 1 The Number of Exploited Units as a Measure of Technology Platform Risk

We use a binomial distribution to model the number of exploited units for each model m_i. Using the Bernoulli mixture approach, we can calculate the unconditional, marginal distribution of Y_i based on Kang et al. (2015):

$$P(Y_i = x) = p_g \binom{N_i}{x} g_i^x (1 - g_i)^{N_i - x}.$$

Beyond assuming that g_i is sufficiently small (see above), we also assume that the number of units of an IoT model N_i is large. To allow for better computability, we thus use the Poisson approximation for a Bernoulli distribution and derive (1) (Kang et al., 2015):[1]

$$P(Y_i = x) \approx p_g \frac{(\lambda_i)^x}{x!} e^{-\lambda_i}, \text{ where } \lambda_i = N_i \cdot g_i. \quad (1)$$

From (1), we obtain the probability that the number of exploited units Y_i for model m_i equals x. For instance, we obtain the probability that $x = 3,000$ units of the D-Link DCS-930L webcam are exploited. The overall designs of two models can be quite similar, for instance, for the D-Link DCS-930L webcam (m_1) and the D-Link DCS-932L webcam (m_2). For these two models, we assume a (high) correlation in case of a TP vulnerability because exploits in one model may indicate the presence of vulnerabilities or corresponding exploits in the other. In contrast, TomTom GO navigation systems (m_3) use the same BusyBox TP, but the exploits between the navigation system and the webcams may only be weakly correlated. A high number of webcams being exploited does not necessarily correlate to a high number of navigation systems being exploited. Further, we interpret two uncorrelated models as using individually designed (i.e., different) TPs. This would be a situation in which the D-Link DCS-930L and D-Link DCS-932L webcams use similar functional units, but on different TPs, i.e., D-Link DCS-930L would use BusyBox, and D-Link DCS-932L would build on another entirely different TP. We can model these correlations in the Bernoulli mixture model between random variables (Bluhm et al., 2010), i.e., in our case, we can model the correlation of dif-

[1] Note that the number of IoT devices can be assumed to be very large. However, to allow for a good approximation of the underlying Bernoulli model by the Poisson distribution, we keep $\lambda_i = g_i N_i$ at a reasonable size. This does not affect our subsequent discussion of governance implications for TP use in IoT because we focus on generalizable insights for fundamentally different scenarios rather than on specific numbers.

ferent models m_i of a platform using a correlation coefficient $\rho_{i,j}$.

We consider a TP with only two models m_1 and m_2 in the following, and we set the exploit probabilities $g_1 = g_2$. This allows us to illustrate the basic connections between the model parameters. Since we focus on deriving governance implications from our model, we point out that the assumptions do not restrict our subsequent insights to a two-model situation. A more general modeling of Bernoulli mixtures can, for instance, be found in Bluhm et al. (2010). Following Bluhm et al. (2010) and Kang et al. (2015), we obtain three cases that depict different correlation levels: the two models can be *partially correlated*, *perfectly correlated*, or *uncorrelated*. To improve readability, we set $\tilde{\rho} = p_g + \rho_{1,2}(1 - p_g)$.

Partially correlated $(0 < \rho_{1,2} < 1)$:

$$P(X_{\text{partially}} = x) = \tilde{\rho} p_g \frac{(\lambda_1 + \lambda_2)^x}{x!} e^{-(\lambda_1+\lambda_2)} + p_g(1 - \tilde{\rho}) \frac{\lambda_1^x e^{-\lambda_1} + \lambda_2^x e^{-\lambda_2}}{x!}. \quad (2)$$

From this general formula, we directly get the two special cases for perfectly correlated ($\rho_{1,2} = 1$, i.e., $\tilde{\rho} = 1$) and uncorrelated models ($\rho_{1,2} = 0$, i.e., $\tilde{\rho} = p_g$):

Perfectly correlated $(\rho_{1,2} = 1)$:

$$P(X_{\text{perfect}} = x) = p_g \frac{(\lambda_1 + \lambda_2)^x}{x!} e^{-(\lambda_1+\lambda_2)}. \quad (2a)$$

Uncorrelated $(\rho_{1,2} = 0)$:

$$P(X_{\text{uncorrelated}} = x) = p_g^2 \frac{(\lambda_1 + \lambda_2)^x}{x!} e^{-(\lambda_1+\lambda_2)} + p_g(1 - p_g) \frac{\lambda_1^x e^{-\lambda_1} + \lambda_2^x e^{-\lambda_2}}{x!}. \quad (2b)$$

Distinguishing these three cases allows us to discuss TP governance choices more distinctly. We will now illustrate the insights from our TP risk model, looking into the different input parameters' effects regarding their impacts on the overall risk for TPs in the IoT. We will further relate our findings to current literature and derive governance implications for the IoT.

4 Application Scenario and Governance Implications for the IoT

From (2)–(2b), we conclude that four distinct parameters impact the risk of exploits for TPs in the IoT. An analysis of these parameters thus allows for a detailed discussion of appropriate IoT governance aspects. We outline how the *correlation* coefficient $\rho_{1,2}$, the *vulnerability probability* p_g, the *exploit probability* g_i, and the *model size* N_i (and, thus, the overall *platform size* consisting of all models), determine the risk of large-scale exploits in the IoT. We use the example of BusyBox (ICS-CERT., 2022) to illustrate and analyze these parameters' impacts based on an application example and analytical insights. We further derive and discuss implications for IoT security governance as a first research step in this direction. In particular, we outline how the use of TPs affects conformity and non-conformity costs (Slaughter et al., 1998) and derive implications for IoT security governance.

We thus distinguish between the *individual*, *company*, and *regulatory* levels of IoT governance measures. At the individual level, we locate the individual end-user that makes use of a smart thing built on a specific TP. At the company level, we see both suppliers who develop and distribute TPs and manufacturers that make use of these TPs when developing their smart things. Finally, the regulatory level involves policymakers, regulators, and authorities who are responsible for setting the rules for TPs use, development, and distribution in the IoT.

4.1 Correlation, Homogeneity, and Heterogeneity

4.1.1 Application Example and Model Implications

We follow a two-step approach when analyzing and discussing our model. First, we provide an application example to illustrate the fundamental properties and outline the differences between correlated and uncorrelated TPs. Note that the expected number of exploits is independent of the degree of correlation and only depends on the other parameters. Second, we look into analytical results to gain deeper insights into the model's parameters and various governance implications. We see that a key question is whether to use a single TP or more than one TP for different models, i.e., deciding for homogeneity or for a specific heterogeneity level. As outlined, we model this by using different correlation levels.

We begin with an application example, for which we assume a *vulnerability probability* $p_g = 10\,\%$. We consider two models m_1 and m_2 with $N_1 = 25,000$ and $N_2 = 25,000$, i.e., a *platform* size of 50,000 units, with exploit probabilities $g_1 = g_2 = 0.1\,\%$. We compare three distinct scenarios: *Scenario A (homogeneity)* – model m_1 (D-Link DCS-930L) and m_2 (D-Link DCS-932L) are perfectly correlated since they both use the BusyBox TP. *Scenario B (partially correlated)* – model m_1 (D-Link DCS-930L) and m_2 (TomTom GO navigation system) use the BusyBox TP but enact in a different environment, such that a partial correlation can be assumed (we use $\rho_{1,2} = 0.5$ for this scenario). *Scenario C (heterogeneity)* – model m_1 (D-Link DCS-930L) and m_2

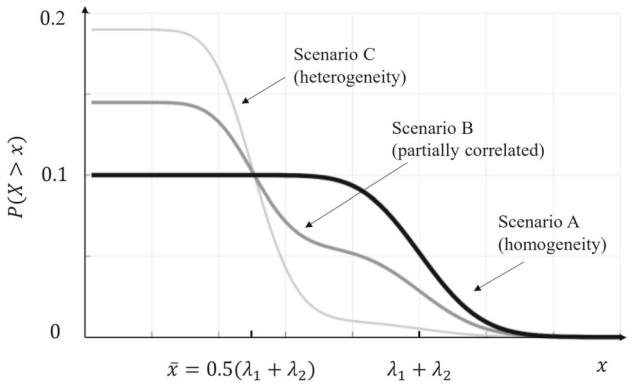

Fig. 2 Risk Measure for Technology Platform Exploits in Different Scenarios

(SmartFrog Cam) are uncorrelated, since only model m_1 uses the BusyBox TP, whereas m_2 uses a different TP without this specific vulnerability.[2] Nonetheless, we assume that the TP of model m_2 (SmartFrog Cam) is affected by another vulnerability with the same vulnerability probability p_g.

Figure 2 illustrates the probabilities $P(X > x)$, i.e., the probabilities for the partially correlated scenario 2, the perfectly correlated scenario 2a, and the uncorrelated scenario 2b. We exemplarily set our threshold $\overline{x}$ that determines a large-scale exploit to $\overline{x} = 0.5(\lambda_1 + \lambda_2)$. Thus, when we refer to large-scale exploits in the following, we mean cases in which the number of exploited units exceeds $\overline{x}$.

For scenarios A, B, and C, the curves represent the probability of more than a certain number of units x being subject to an exploit. Notably, we are less interested in the exact number of exploited units than in the differences between the scenarios. The different scenarios yield different results. A small number of exploited units ($x < \overline{x}$) is most likely in scenario C, i.e., for two individually designed TPs. Since the TPs for D-Link DCS-930L and the SmartFrog Cam are distinct and, therefore, do not have the same set of vulnerabilities, they can be exploited differently. Thus, chances are that either of these two models will experience an exploit. This is more likely compared to the case of a single TP (e.g., for both D-Link DCS-930L and D-Link DCS-932L) experiencing an exploit (scenario A). Applying the same logic, it is coherent that the probability in scenario C drops quickly when the number of exploited units increases because each of the TPs only represents 50 % of the overall platform size, whereas in scenario A, the TP represents 100 % of the overall platform size. For scenario B, the probability of a small number of exploited units is larger than it is for platform homogeneity (scenario A), but lower compared to two entirely uncorrelated models (scenario C). Likewise, the probability for large-scale exploits in scenario B decreases slower than for heterogeneous TPs (scenario C) and faster than for perfectly correlated models (scenario A). Looking in detail into the analytical results, Kang et al. (2015) used (2) to show the following relationship for large x (note that x is naturally bounded by $N = N_1 + N_2$):

$$\lim_{x\to\infty} \frac{P(X_{\text{partially}} > x)}{P(X_{\text{uncorrelated}} > x)} = \frac{\rho_{1,2}}{p_g} + (1 - \rho_{1,2}). \tag{3}$$

In particular, we obtain the special case for $\rho_{1,2} = 1$:

$$\lim_{x\to\infty} \frac{P(X_{\text{perfect}} > x)}{P(X_{\text{uncorrelated}} > x)} = \frac{1}{p_g}. \tag{3a}$$

Equation (3a) is particularly interesting since it generalizes our comparison of the scenarios A and B with C for $x \to \infty$. (3a) also implies that using one TP (scenario A) is $1/p_g$ times as risky as using two uncorrelated TPs (scenario C). In addition, for $x > \lambda_1 \geq \lambda_2$, the distribution for the correlated case drops steeply around $\lambda_1 + \lambda_2$, and the tail probabilities quickly approach the limit (Kang et al., 2015).

The ratio between the partially correlated (scenario B) and uncorrelated (scenario C) case depends on the correlation coefficient $\rho_{1,2}$ (cf. (3a)). The greater the correlation, the higher the relative difference in the two cases for $x \to \infty$. In our scenarios, this implies that the higher the correlation coefficient, the riskier scenario B is compared to scenario C. The interpretation is straightforward: Since D-Link DCS-930L and TomTom GO navigation system use the BusyBox TP, they may have the same vulnerability. Yet, both models are part of a different software ecosystem and utilize different hardware components and interfaces, among others. The more the surrounding environment of the TP differentiates the two models from each other (smaller $\rho_{1,2}$), the less likely that both models experience a large number of exploited units caused by this vulnerability concurrently because more adjustments are necessary to exploit the vulnerability. In sum, we gain two main TP characteristics (TPCs) concerning correlation, homogeneity, and heterogeneity:

TPC I: It is more likely for the two-TP case (scenario C – heterogeneity) than for the one-TP case (scenario A – homogeneity) to experience any exploit, i.e., an exploit in at least one unit.

TPC II: Large-scale exploits are more likely for the one-TP case (scenario A – homogeneity).

4.1.2 Implications on Technology Platform Governance

From the above TPCs, we conclude that the choice of how many and which TPs shall be used represents a strategic decision owing to the risk implications of correlation between the

[2] Smartfrog Ltd. (2012) lists no visible reference to the open-source BusyBox TP.

models of a TP. Thus, such a decision can enable the avoidance of frequent over-investments in homogeneity (yu Chen et al., 2011).

We do not see an effective way to influence the correlation of models at the *individual level*. In most cases, end-users will probably neither know which TPs they use nor could they get simple instructions on how to act accordingly. At the *company level*, we integrate the implications of model correlation in the distinction between *costs for conformity* (i.e., expenditures associated with the identification and prevention of vulnerabilities) and *costs of non-conformity* (i.e., expenditures for reworking, maintenance, liability damages, or litigation) (Slaughter et al., 1998). TPs in the IoT generally require a trade-off between costs for conformity to increase TPs' security levels and costs of non-conformity to bear the consequences in the case of an exploit. Thus, we find ourselves in the role of the sorcerer's apprentice: to choose between discretion and valor for TPs in IoT.

Facing TPC I and TPC II, companies may find themselves torn between the tension between homogeneity and heterogeneity because the risk and its associated implications for companies change depending on the extent of an exploit (cf. intersection at $x \approx 0.5 \cdot (\lambda_1 + \lambda_2)$ in Fig. 2). In scenario A (homogeneity), the risk of large-scale exploits should motivate companies to invest in conformity, since the non-conformity costs of an exploit are potentially enormous (TPC II). Non-conformity costs of fixing the vulnerability in circulating and future smart things, compensation claims, legal expenses, image loss, and a drop in future sales can occur. In scenario C (heterogeneity), large-scale exploits and their negative effects are less likely. Yet, conformity costs potentially scale with the number of TPs being used, as every TP has its own vulnerabilities that companies must take care of (TPC I). Thus, and in line with prior IS research, it is a strategic decision to consider how many models should be based on the same TP and to compare conformity costs and non-conformity costs with the costs of developing or using an additional TP (yu Chen et al., 2011; Temizkan et al., 2017). Scenario B, therefore, becomes an important and nuanced option to choose a suitable TP, since it may tend to favor scenario A ($\rho_{1,2} > 0.5$) or scenario C ($\rho_{1,2} < 0.5$).

Here, the question arises for *suppliers* how many models are based on their TP, since this has implications for the risk and associated costs. In the context of the IoT, it becomes increasingly complex to trace the usage of TPs owing to the modularity of hardware and software components. The case of BusyBox illustrates that devices of very different shapes and functions can use the same TP, without any influence the supplier could exert. Thus, the decision between homogeneity and heterogeneity shifts – in part to – the *manufacturer*. For instance, webcam manufacturers using BusyBox in their smart things have the choice of whether to base all of their models on BusyBox (homogeneity) or whether to use different TPs for different models. Besides the choice between existing TPs, manufacturers could also choose to develop their own TP, which would constitute an individual TP design. This ambivalence in terms of open-source versus proprietary software and the concept of *security by obscurity* (i.e., an increased security level owing to proprietary design) is in line with the IS literature (West, 2003; Economides & Katsamakas, 2006; Boulanger, 2005).

As such, manufacturers face a continuum of choices, ranging from mere platform adoption to platform adoption with potentially security-relevant modifications to an individual design to influence the correlation of the models involved. At the *regulatory level*, the question arises how much platform homogeneity or heterogeneity should be allowed and enforced. This relates to similar discussions of software diversity, for instance, regarding antitrust law and technology standards (yu Chen et al., 2011). Yet, proprietary platforms oppose the vision of an IoT with open interfaces and a high degree of connectivity (Keoh et al., 2014). We see two possible paths for regulation: On the one hand, regulators could engage in strict legal requirements, using correlation among models as indicators for TPs with widespread distribution and could focus regulatory action accordingly. For instance, political action could impose quotas for TP use, restrictions for TP adoption and adaptation, or conditions for conformity costs. On the other hand, policymakers could refrain from any regulatory action on homogeneity or heterogeneity and could leave the decision of correlation among models to the companies. Desirable action could be incentivized by designing appropriate consequences: positive (e.g., certifications) and negative (e.g., costs of non-conformity).

The strategic decision within the continuum between homogeneity and heterogeneity and the associated governance measures for model correlation is important to manage the risk of TPs in the IoT. As illustrated, the risk also depends on the vulnerability probability p_g as well as the expected number of exploited devices (i.e., the product of exploit probabilities and platform sizes: $\lambda_i = g_i \cdot N_i$). Thus, we will discuss these parameters' influences in more detail in the following sections.

4.2 Vulnerability Probability and Conformity Costs

4.2.1 Model Implications

We will now outline how a change in the *vulnerability probability* p_g influences the risk of exploits and how this can affect the governance of TPs. From (3), we derive an interpretation that may seem counter-intuitive at first glance: The risk ratio for perfectly correlated TPs and uncorrelated TPs converges to $1/p_g$ for $x \to \infty$. Thus, other model parameters (i.e., model sizes and exploit probabilities) do not influence this

ratio. This means that the smaller the vulnerability probability p_g, i.e., the more secure the TP is in general, the riskier the use of one TP compared to the use of two uncorrelated TPs is in relative terms. For instance, scenario A is 10 times riskier than scenario C in our application example, where $p_g = 10\,\%$. Assuming a lower vulnerability probability of $p_g = 1\,\%$ (ceteris paribus), scenario A is 100 times riskier than scenario C. Thus, although not in absolute but in relative terms, using one TP instead of using two becomes comparatively riskier with decreasing vulnerability probability p_g. We thus derive the following TPCs concerning vulnerability probability:

TPC III: For $x \to \infty$, the relationship between scenarios A and C solely depends on the vulnerability probability p_g.

TPC IV: For $x \to \infty$, the lowering of the vulnerability probability p_g makes the use of one TP relatively riskier compared to two uncorrelated TPs.

As noted, we consider the vulnerability probability as given ex-ante in our model. However, further development of the TP may necessitate a re-evaluation of p_g. For instance, owing to technological developments, the TP also develops further. Thus, the underlying TP design changes and new vulnerabilities emerge, or existing vulnerabilities disappear. It is then reasonable to assign these new circumstances to the TP's vulnerability probability. One may argue that this could be interpreted as a new or different TP; however, we consider the gradual change over time as more intuitive for TPs in the IoT with common software updates. Referring to our application examples, a new release for BusyBox may change the TP for the D-Link DCS-930L, the D-Link DCS-932L, the TomTom GO navigation system, and others. While this release may both remove existing vulnerabilities and introduce new vulnerabilities in the TP, the exploit probability is subject to the specific usage environments of smart things (cf. Kang et al., 2015). Thus, the exploit probability may not change as long as the usage scenario of the smart thing (e.g., usage intensity or user behavior) remains unchanged.

We further analyze (2) to investigate the effects of changes for p_g, since (2a) and (2b) constitute special cases of (2). We do this by analyzing both summands of (2) and how a change in p_g affects each summand. In (2), the two summands

$$\frac{(\lambda_1+\lambda_2)^x}{x!}e^{-(\lambda_1+\lambda_2)} \quad \text{and} \quad \frac{\lambda_1^x e^{-\lambda_1}+\lambda_2^x e^{-\lambda_2}}{x!}$$

represent Poisson distributions with parameters $\lambda_1+\lambda_2$, λ_1, and λ_2, respectively. Each of them only contributes non-negative values for all x. The vulnerability probability p_g contributes to $\tilde{\rho}\,p_g$ and $p_g(1-\tilde{\rho})$ of (1), where $\tilde{\rho} = p_g + \rho_{1,2}(1-p_g)$. Since the first term

$$\tilde{\rho}\,p_g = p_g^2 + \rho_{1,2}p_g - \rho_{1,2}p_g^2$$

is monotonically increasing for $p_g \in (0,1)$, increasing p_g increases the first summand of (1). Further, $p_g(1-\tilde{\rho}) = (\rho_{1,2}-1)p_g^2 + (1-\rho_{1,2})p_g = (\rho_{1,2}-1)p_g(p_g-1)$ is a negative quadratic function in p_g with maximum in $p_g = 0.5$. Thus, increasing p_g within the open interval $(0, 0.5)$ also increases the second summand of (2); i.e., both summands increase. As noted, we assume the vulnerability probability to be small to moderate. Therefore, $p_g \in (0.5, 1)$ is a scenario we consider unrealistic since it would imply that the TP is assumed to have a vulnerability probability by design with more than 50 % chance. Thus, we do not provide a detailed analytical analysis for this case. In effect, an increased vulnerability probability directly increases the risk of TP use. We derive the following TPCs concerning vulnerability probability:

TPC V: An increased vulnerability probability directly increases the risk of TPs in the IoT.

From these model implications, we conclude there is a high relevance of vulnerability probability for TP risk in IoT. In particular, TPC III underlines this argument for $x \to \infty$, and TPC V in general. Referring to the costs related to software quality (Slaughter et al., 1998), *costs for conformity* are the major influencing factor to alter the vulnerability probability. Because a vulnerability prevails by design (and is unknown ex-ante), a lowered vulnerability probability can be achieved via increased conformity costs, to a certain extent. Thus, measures should be taken to avoid vulnerabilities in the first place and to help ensure that not only a specific exploit is addressed, which would constitute costs of non-conformity.[3] We argue that governance measures to decrease vulnerability probability should focus on costs for conformity, so as to disclose and address vulnerabilities before an exploit occurs.

4.2.2 Implications on Technology Platform Governance

Similar to the correlation between TP models, it is almost impossible to influence the probability of a TP vulnerability at the *individual level*. Nonetheless, individuals should be aware of TPs and their potential vulnerabilities. Thus, educating end-users to value security and to pay close attention

[3] Notably, costs for conformity may result in internal costs of non-conformity (e.g., for reworking or retesting) before an exploit has occurred (Slaughter et al., 1998). Nonetheless, we focus on costs for conformity in our reasoning because they induce an appropriate response to the vulnerability.

to signals of TP security efforts (e.g., certifications) (Eltayeb, 2017) may be a beneficial measure. Since end-users can barely affect the vulnerability probability, there is a strong need for companies and regulators to reduce the vulnerability probability by means of effective governance measures.

A *supplier* of a specific TP should be incentivized to provide a TP with low vulnerability probability to avoid the negative effects of TPC V. Otherwise, potential costs of non-conformity pose a substantial threat to suppliers owing to the vulnerability probability's direct effect on TP risk. This could comprise costly recalls, updates, or bad publicity in case of an exploit. To effectively manage a TP's vulnerability probability, suppliers should use security standards (e.g., effective encryption), even though it may negatively affect responsiveness and battery life (Neville-Neil, 2017), audits, security by design (i.e., the focus on security during development), and code testing (e.g., penetration tests or competitions such as Google Pwnium and Project Zero). For instance, in the case of Spectre and Meltdown, Google's Project Zero proved to be an effective instrument for vulnerability detection and exploit prevention (Linton & Parseghian, 2018). For the purpose of testing, suppliers can use different testing procedures, such as static (i.e., procedures during development and testing), dynamic (i.e., procedures during the operation by simulating an attack), and interactive (i.e., an agent-based behavioral analysis for simulated attacks) application security testing, drawing from internal or external resources (Lemos, 2024).

Although *manufacturers* of smart things might face negative effects in case of a TP-based exploit, it may be difficult – if not impossible – for them to influence the vulnerability probability because a manufacturer often just applies a previously designed TP and is not directly accountable for it. Yet, a manufacturer can take measures regarding the application of the TP in its own smart things. For instance, manufacturers should engage in structured TP selection processes that evaluate the probability of vulnerabilities before adopting a TP for their smart things. Such a conscious selection would also include considerations about platform homogeneity and heterogeneity (cf. Section 4.1). Further, manufacturers should consider the complex interdependence between the TP and other components of a smart thing as well as multiple interfaces.

At the *regulatory level*, standards for TPs in the IoT should be defined to avoid situations in which companies make excessive conformity cost savings at the expense of a higher vulnerability probability or at the expense of non-conformity costs in the case of an exploit (Lee et al., 2016). Axelrod (2015) points out that suppliers often lack the motivation to ensure that devices are "secure, safe and have sufficient privacy protection" (cf. Axelrod, 2015, p. 2). Suppliers should be held responsible for building secure, safe, and privacy-preserving systems (Axelrod, 2015; Sicari et al., 2016). This situation must be addressed in politics and by regulators, particularly for any TP used in critical infrastructure (e.g., smart grids). For instance, the Federal Trade Commission (FTC) filed a complaint against the United States (US) subsidiary of the Taiwan-based network equipment provider D-Link for taking inadequate security measures and putting consumers' privacy at risk (Federal Trade Commission., 2017), trading lower conformity costs for a higher vulnerability probability (Violino, 2017). A challenge in this context is that – while TPs are often global – political influence is mostly limited to a geographical region.

In an increasingly connected and platform-based future, political structures are required to go beyond borders and define standards, regulations, and emergency plans locally, regionally, and globally. This is a demanding effort, since a global institution and a holistic legal approach would be necessary to achieve such a goal (Karale, 2021). To not exceed this paper's scope, we refer to Karale (2021) for more details on legal frameworks for the IoT. However, the incentives for suppliers must be increased so as to ensure a low-vulnerability probability (Hampson, 2019). Policymakers could achieve this by imposing fines on companies that make TPs with low security standards available. Initiatives like the EU's General Data Protection Regulation (GDPR), Regulation EU 2016/679. (2016), implemented in 2018, and the NIS 2 Directive (EU) 2022/2555 (2022) that came into effect in 2023, as well as the recently proposed revision of the EU's Product Liability Directive (COM/2022/495 final, 2022) that is expected to incorporate software components and, therefore, IoT devices, are steps in this direction. They require measures such as responsible disclosure as well as reporting and dissemination obligations in case of vulnerabilities, which increase the suppliers' incentive to invest in costs for conformity. Such regulation is necessary as otherwise, chances are that companies will aim at low conformity costs at the expense of customers' security and potential non-conformity costs. Yet, such regulation in the context of the IoT is rare, and there is little guidance on the specifics of TPs in the IoT.

Although the proposed governance measures to decrease the vulnerability probability have a direct and positive (i.e., mitigating) impact on the risk of TPs in the IoT, they alone are insufficient. As we see in TPC IV, decreasing the vulnerability probability can even complicate the situation for decision-makers, since the risk ratio between correlated and uncorrelated models changes depending on the degree of correlation between the models of a TP. Thus, companies and regulators should strive for an integrated approach in combination with the governance implications from Section 4.1. We will now extend our argument for an integrated risk management approach of TPs in IoT with the exploit probability and model size.

4.3 Exploit Probability, Model Size, and Non-Conformity Costs

4.3.1 Model Implications

With $\lambda_i = N_i \cdot g_i$ being the expected value of the Poisson distribution, an increase in either the exploit probability g_i or the model size N_i increases λ_i. Looking at Fig. 2, this means shifting the curves to the right. Thus, we derive the following TPC:

TPC VI: Increasing the exploit probability or the model size increases the probability $P(X > x)$, especially for large-scale exploits ($x > \overline{x}$).

In other words, a higher exploit probability increases the probability of large-scale exploits. The same holds true for an increased model size. Intuitively, more existing units of a model increase the probability of more units being exploited in absolute numbers. Further, TPC VI indicates that exploit probability and model size must be considered jointly. For instance, TP models with a small number of units may have a higher exploit probability compared to other TPs with bigger model sizes, yet resulting in the same overall risk (ceteris paribus).

4.3.2 Implications on Technology Platform Governance

Once a vulnerability manifests, the consequences become palpable for all smart things built on the same TP. One frightening example was the impact of the WannaCry attack on more than 40 hospitals operated by the National Health Service in the United Kingdom (Medeiros, 2017). Following this attack, many hospitals stopped operation and patients had to be moved to unaffected hospitals. Despite the concerning and often unforeseeable consequences of such TP exploits, there are effective countermeasures to avoid many of the common threat scenarios. However, such countermeasures imply costs of non-conformity, which can be subdivided into those related to *internal failure* and *external failure* (Slaughter et al., 1998). Internal failure non-conformity costs correspond to costs that occur before a product (in our case, the TP) is distributed, whereas external failure non-conformity costs emerge from failures after a unit has been delivered to the customer (Slaughter et al., 1998). We now discuss potential governance measures relating to costs of non-conformity.

For *individuals* and *manufacturers*, it is advisable to regularly update all their smart things. As simple as this may seem, users' behavior and their security awareness are critical factors in IT security management (Colwill, 2009; Frank et al., 2022). Further, security checks and standards should be implemented with the same rigor as for any other IT components. This would also require individuals and manufacturers to regularly monitor their smart things for unusual behavior, for instance, to detect whether their refrigerator is part of a botnet and is, therefore, sending server requests with high frequency. Manufacturers using TPs in the IoT need to implement effective measures to mitigate security incidents to maintain their competitive edge. Yet, such unusual behavior may be hard to detect and the measures may be too complicated to be carried out by individuals and manufacturers alone.

Although vulnerabilities cannot be ruled out, since they usually become visible ex-post, exploits' effects can be restricted, which causes external failure non-conformity costs, particularly for *suppliers*. Thus, most of the responsibility to limit exploits lies with the TP supplier. For TPs in the IoT, two cases can be distinguished once an exploit occurs: a physical malfunction and a software malfunction. Both cases may also be interrelated. For physical malfunctions, recalls are the most likely option for repair, whereas software vulnerabilities' effects may be handled depending on the specific exploit, often by providing patches. In the case of a recall, the larger the platform size is, the higher the non-conformity costs. Thus, suppliers should strive for patches without being required to physically turn in their smart thing (e.g., Tesla over-the-air updates) (York, 2018). While this reduces non-conformity costs, one must bear in mind that such an additional interface constitutes a risk on its own.

We argue that the exploit probability increases over time, since once a security breach goes public, the number of exploited units and copycats will also increase. Thus, it is crucial to provide timely security updates. In light of the preceding discussion, this also implies that physical vulnerabilities are the more critical ones, since fixing them requires (on average) more time and effort. In effect, such vulnerabilities provide a longer period of insecurity and entail higher costs. Because suppliers do not always have incentives to quickly provide patches, governance actions such as service-level agreements between individuals or manufacturers and suppliers, cost-sharing, or liability may be appropriate measures to incentivize short patch times (Cavusoglu et al., 2008).

Particularly for TPs used in critical infrastructures, guidelines for patch times, update cycles, or similar should be considered and defined at the *regulatory level*. However, the suppliers of a TP in IoT may consider trading conformity costs for non-conformity costs, gambling on the non-occurrence of non-conformity costs. For instance, before increasing the recurring costs for internal auditing processes, a company may accept the potentially occurring non-conformity costs of a recall or necessary software update in the future. This strategy will often come at the expense of their customers' security, i.e., at the expense of manufacturers or individuals. Thus, a regulatory framework must be defined to prevent or prosecute such strategic decisions at the expense of others. One way to achieve this would be an artificial increase of the

non-conformity costs by means of fines, mandatory recalls, compensation of the affected platform's users, and the like. Further, regulators could also engage in cyber-defense and IT security consultancy activities for the IoT. For instance, the Industrial Control Systems Cyber Emergency Response Team provides alerts, advisories, assessments, and training for security incidents (Cybersecurity & Infrastructure Security Agency., 2024). Other government institutions identify vulnerable IoT devices to motivate individuals to take preventive security measures (Ministry of Internal Affairs and Communications, National Institute of Information and Communications Technology., 2019). Finally, the question of product liability is of high importance for non-conformity costs and should be addressed by regulators (Lee et al., 2016). In fact, the European Union's Product Liability Directive that includes hardware and software aspects of smart devices (COM/2022/495 final, 2022) may be a valuable step in this direction. Clear responsibilities are needed to minimize the negative effects of exploits, i.e., who is responsible: the supplier as the designer of the TP and its vulnerability, or the manufacturer as the direct contact person? While suppliers cannot control the various application areas of their TPs, individuals are often left to deal with the consequences.

4.4 A Note on Technology Platform Connectivity in the IoT

As outlined above, our model of TP use in the IoT provides guidance concerning influencing factors for TP security risks but cannot explicitly account for the impacts of the connectivity level within a TP. Imagine a situation in which an exploit hops from one smart thing to another, for instance, enabled by over-the-air updates or communication interfaces. Since these cascade effects can have very low thresholds to become an epidemic in real networks (Prakash et al., 2012), cascades may lead to a continuously increasing number of exploited units owing to rapid spreading hazards 'from thing to thing'. With this risk in mind, a high intra-network and inter-network connectivity may increase the number of exploited units and, therefore, a TP vulnerability's impacts. This risk can be amplified by the aforementioned homogeneity of platforms, whereby exploits of one smart thing are easier to transfer to other things. Both connectivity and homogeneity aspects are interrelated, also with the overall platform size. However, these parameters are defined, among others, by technological trends, communication and interaction paradigms, and market trends in the IoT ecosystem. Individuals, companies, and regulators have limited control over these factors. Nonetheless, reflections on the impact of connectivity and homogeneity, as well as their interplay with platform size, are important to structure effective governance actions for IoT.

Individuals should be as careful and proactive using any IoT devices as they would be making sure their home, personal computer, tablet, or mobile phone is always locked and secure, as failures can even threaten human lives (Sadeghi et al., 2015). Because the boundaries between the physical and the digital world are blurring, comprehensive security measures that include all aspects of cyber-physical systems and digital environments are advised (Ransbotham et al., 2016). To prevent cascading exploits, manufacturers should implement various measures to secure interfaces and to enable secure connectivity, such as, among others, access control policies, hardware security modules, and software update management (Keoh et al., 2014). For a detailed discussion of specific security threats, we refer to the literature. For instance, Sadeghi et al. (2015) provide a detailed outline of the security and privacy challenges relating to industrial IoT systems and suggest a holistic security framework.

Suppliers and regulators have much the same options as manufacturers by strengthening the security of communication protocols and/or creating legal requirements for secure connectivity. They could also take IoT governance a step further by explicitly restricting connectivity between smart things or the platform size. For instance, a maximum quota of similar devices or a minimum deviation degree between models could represent sensible governance actions. Beyond this, many organizations implement additional security measures such as the use of virtual private networks (VPNs), firewalls, and the zero trust model (Buck et al., 2021). Yet, while such measures may be tempting at first glance, they do not necessarily capture the full extent of the above-mentioned exogenous factors of the IoT ecosystem comprehensively.

5 Conclusion

TPs in the IoT evolve rapidly. Unfortunately, governance is frequently unable to keep pace with technological development. The physical and digital worlds are becoming increasingly interconnected, and smart things are inheriting risks previously reserved for software artifacts. Recently, many IoT security breaches have substantially affected individuals, companies, and (governmental) organizations in various applications. To model the risks of exploits of such TPs, we transferred Kang et al. (2015)'s platform risk approach to IoT TPs. Using the application example of BusyBox, we discussed key influencing parameters of IoT TP security risks. In particular, we identified *correlation, vulnerability probability, exploit probability, model and platform size*, as well as *connectivity* as relevant parameters to guide IoT governance decisions.

We discussed these parameters' impacts on TP risk as well as their interdependencies with conformity costs and

non-conformity costs to derive governance implications for TP use in the IoT. We found that companies should carefully consider their TP heterogeneity level since experiencing at least one exploit is more likely for two uncorrelated models (TPC I), whereas large-scale exploits are more likely for homogeneous TPs (TCP II). Vulnerability probability is influential since it directly translates to an increased or decreased risk (TPC V). Further, for $x \rightarrow \infty$, the ratio between TP homogeneity and heterogeneity depends on the vulnerability probability (TPC III) alone, and homogeneous TPs become riskier compared to heterogeneous ones settings when decreasing the vulnerability probability (TPC IV). The exploit probability and model size mainly affect large-scale exploits (TPC VI).

We also identified several potential governance measures at the individual, company, and regulatory levels relating to the TPCs. From the individual perspective, IoT TPs are often not apparent, limiting the potential governance measures to increased awareness for security, for instance, by ensuring regular updates. Supplier companies may limit the level of conformity costs, trading it for potential non-conformity costs, partially owing to the absence of effective regulation, since it has no inherent value until a (relatively unlikely) exploit occurs. Since manufacturers can hardly avoid using TPs owing to their functional and economic benefits, they should establish good governance practices such as structured TP selection, timely patches, or audits. Thus, we argue for a deliberate, strategic decision-making process by manufacturers on the interfaces and connectivity levels of their smart things (Thielmann, 2017), considering the appropriate – or, rather, necessary – platform security level. Yet, it is hard to engage in the IoT governance field from companies' perspectives if regulation provides no effective framework or responsibilities for regulation are even denied (Thielmann, 2017). Thus, we see a need for increased collaboration at the company and regulatory levels to find an appropriate balance between regulation and open interfaces of IoT, i.e., conformity and non-conformity costs. This is especially challenging considering the requirement for international regulation frameworks owing to the global nature of the IoT (Weber, 2010; Nicolescu et al., 2018). Combining our model interpretation with the notion of epidemic thresholds, we

Table 2 Technology Platform Characteristics and Security-Related Governance Measures

TPC	Description	Governance Implications
I-II	It is most likely for the uncorrelated case (scenario C – heterogeneity) and least likely for the perfectly correlated case (scenario A – homogeneity) to experience an exploit at all, i.e., an exploit in at least one unit. Large-scale exploits are most likely for the perfectly correlated case (scenario A – homogeneity) and least likely for the uncorrelated case (scenario C – heterogeneity).	At the *individual* level, it appears largely impossible to influence the correlation of models. *Companies* may have to make a strategic decision to resolve tensions between model homogeneity and heterogeneity. *Suppliers* will have to identify how many models are based on their TP. *Manufacturers* will face a continuum of choices. At the *regulatory* level, a decision may have to be made to which extent TP homogeneity and heterogeneity would be desired and enforced.
III–V	For $x \rightarrow \infty$, the relationship between scenarios A and C solely depends on the vulnerability probability p_g. For $x \rightarrow \infty$, the lowering of vulnerability probability p_g makes the use of one TP relatively riskier compared to two uncorrelated TPs. An increased vulnerability probability directly increases the risk of large-scale exploits of TPs in IoT.	At the *individual* level, it appears largely impossible to influence the correlation of models. Individuals should be aware of the TPs used and their vulnerabilities. *Companies* and *regulators* may thus have to step in to protect end-users. *Suppliers* should be incentivized to provide TPs with low vulnerability probabilities to manage the risks caused by TPC V. They may also rely on the use of established security standards, audits, security by design, and code testing. As *manufacturers* apply previously designed and supplied TPs, they have limited control over vulnerabilities. Nevertheless, they are incentivized to do their best when it comes to the selection of TPs and the related security audits. At the *regulatory* level, legal requirements and norms could be developed to avoid situations in which companies aim to achieve excessive conformity cost savings at the expense of higher levels of vulnerability.
VI	Increasing the exploit probability or the model size increases the probability $P(X > x)$, especially for large-scale exploits ($x > \overline{x}$).	For *individuals* and *manufacturers*, it is advisable to keep all smart things regularly updated. Most of the responsibility to limit exploits lies with the TP *supplier*. At the *regulatory* level, legal requirements and standards could be formulated, particularly in relation to critical infrastructures.

emphasize the impacts resulting from widespread IoT TP use and potential cascade effects within a highly interconnected IoT. We summarize the different potential governance measures relating to their respective TPCs in Table 2.

Our research has several limitations, which may also stimulate further research on IoT TPs in at least five key areas. First, we focus on generic TP risks, so our governance implications require further elaboration for specific application fields or geographical regions. Future research could focus on a detailed IoT platform governance framework, taking the cause-and-effect-relationships from our paper as a theoretical foundation. Second, our model of TP risks in the IoT represents only an abstract image of complex realities, neglecting additional influencing factors. For instance, we have simplified interfaces, connectivity, model-specific platform adaptations, or inter-temporal facets. This opens promising avenues concerning the validation of our insights with extensive real-world datasets and making them more case-specific; for instance, assessing the severity of vulnerabilities/exploits and adjusting countermeasures accordingly (Cavusoglu et al., 2008). Third, we used a Poisson approximation for the binomial distribution, which limits our model's applicability; other approximations may allow for a better applicability for real-world numbers in future research. Fourth, the explicit analysis of cascade effects in the IoT, for which the Bernoulli mixture model and our notion of correlation may be too simplistic, should be subject to future research. Fifth, our illustrative example focuses on two TPs in the IoT. Future research could thus expand on the model by including more than two TPs and conduct sensitivity analyses for cases in which the Poisson approximation does not hold.

While it remains to be seen who will tame smart things and prove to be the sorcerer in 'IoT Fantasia', we provide initial evidence on promising governance measures. Thus, we contribute to the descriptive body of knowledge by describing TP use in the IoT as well as the associated risks. By transferring a risk quantification approach from the automotive industry, we shed light on the implications on governance choices related to (non-) conformity on security threats in the IoT and thereby explore "the underlying causal structure of the theory" (cf. Meredith et al., 1989, p. 303). We outline which parameters of TPs affect the risks of TP use in the IoT, using the case of BusyBox as an example. Further, we delineate prescriptive governance implications resulting from the parameters of TPs in the IoT. Thus, we help reveal the relevant cause-and-effect relationships that individuals, companies, and regulators can incorporate for sound risk assessments.

Acknowledgements This research was funded in part by the Luxembourg National Research Fund (FNR) and PayPal, PEARL grant reference 13342933/Gilbert Fridgen, as well as grant reference 16326754/PABLO. Supported by Banque et Caisse d'Épargne de l'État, Luxembourg (Spuerkeess). For the purpose of open access, and in fulfillment of the obligations arising from the grant agreement, the authors have applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any Author Accepted Manuscript version arising from this submission.

Author Contributions **Martin Brennecke**: Conceptualization, validation, data curation, writing – original draft, writing – review and editing, project administration. **Gilbert Fridgen**: Conceptualization, resources, writing – review and editing, supervision, funding acquisition. **Jan Jöhnk**: Conceptualization, methodology, validation, formal analysis, data curation, writing – original draft, writing – review and editing, visualization, project administration. **Sven Radszuwill**: Conceptualization, methodology, validation, formal analysis, data curation, writing – original draft, writing – review and editing, visualization. **Johannes Sedlmeir**: Conceptualization, validation, data curation, writing – original draft, writing – review and editing, supervision.

Funding Open Access funding enabled and organized by Projekt DEAL.

References

Aftergood, S. (2018). Governments want your smart devices to have stupid security flaws. *Nature, 560*(7720), 550–551. https://doi.org/10.1038/d41586-018-06033-9

Almeida, V. A., Doneda, D., & Monteiro, M. (2015). Governance Challenges for the Internet of Things. *IEEE Internet Computing, 19*(4), 56–59. https://doi.org/10.1109/MIC.2015.86

Alter, S. (2019). Making sense of smartness in the context of smart devices and smart systems. *Information Systems Frontiers, 9*(4), 381–393. https://doi.org/10.1007/s10796-019-09919-9

Arentz, S. (2005). Hacking Linux-powered devices. Retrieved March 25, 2024, from http://bofh.nikhef.nl/events/CCC/congress/21c3/papers/136%20Hacking%20Linux-Powered%20Devices.pdf

Arnold, L., Jöhnk, J., Vogt, F., & Urbach, N. (2022). IIoT platforms' architectural features - a taxonomy and five prevalent archetypes. *Electronic Markets, 32*(2), 927–944. https://doi.org/10.1007/s12525-021-00520-0

Arora, A., Krishnan, R., Telang, R., & Yang, Y. (2010). An empirical analysis of software vendors' patch release behavior: impact of vulnerability disclosure. *Information Systems Research, 21*(1), 115–132. https://doi.org/10.1287/isre.1080.0226

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Axelrod, C.W. (2015). Enforcing security, safety and privacy for the Internet of Things. In: *Long Island Systems, Applications and Technology*https://doi.org/10.1109/LISAT.2015.7160214

Baldwin, C.Y., & Woodard, C.J. (2008). The architecture of platforms: a unified view. *Harvard Business School Finance Working Paper*, (09-034) https://doi.org/10.2139/ssrn.1265155

Bandyopadhyay, K., Mykytyn, P. P., & Mykytyn, K. (1999). A framework for integrated risk management in information technology. *Management Decision, 37*(5), 437–445. https://doi.org/10.1108/00251749910274216

Bhat, M.I., & Giri, K.J. (2021). Impact of computational power on cryptography. In: K. J. Giri, S. A. Parah, R. Bashir, & K. Muhammad (Eds.), Multimedia security: Algorithm development, analysis and applications (pp. 45–88). https://doi.org/10.1007/978-981-15-8711-5_4

Biswas, B., Mukhopadhyay, A., Bhattacharjee, S., Kumar, A., & Delen, D. (2022). A text-mining based cyber-risk assessment and mitigation framework for critical analysis of online hacker forums. *Decision Support Systems, 152*, 113651. https://doi.org/10.1016/j.dss.2021.113651

Biswas, B., Mukhopadhyay, A., Kumar, A., & Delen, D. (2023). A hybrid framework using explainable AI (XAI) in cyber-risk management for defence and recovery against phishing attacks. *Decision Support Systems., 177*, 114102. https://doi.org/10.1016/j.dss.2023.114102

Bluhm, C., Overbeck, L., & Wagner, C. (2010). *An introduction to credit risk modeling*. Chapman

Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications,54*,. https://doi.org/10.1016/j.comcom.2014.09.008

Boulanger, A. (2005). Open-source versus proprietary software: Is one more reliable and secure than the other? *IBM Systems Journal, 44*(2), 239–248. https://doi.org/10.1147/sj.442.0239

Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security, 110*, 102436. https://doi.org/10.1016/j.cose.2021.102436

Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., & Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. *Nature, 464*, 1025–1028. https://doi.org/10.1038/nature08932

BusyBox. (2022). The swiss army knife of embedded Linux: Products. Retrieved March 25, 2024, from https://www.busybox.net/about.html

Cavusoglu, H., Cavusoglu, H., & Zhang, J. (2008). Security patch management: Share the burden or share the damage? *Management Science, 54*(4), 657–670. https://doi.org/10.1287/mnsc.1070.0794

CISA. (2021). Statement from CISA Director Easterly on Log4j Vulnerability. Retrieved March 25, 2024, from https://www.cisa.gov/news-events/news/statement-cisa-director-easterly-log4j-vulnerability

Chen, P.-Y., Kataria, G., & Krishnan, R. (2011). Correlated failures, diversification, and information security risk management. *MIS Quarterly, 35*(2), 397–422. https://doi.org/10.2307/23044049

Colwill, C. (2009). Human factors in information security: The insider threat- who can you trust these days? *Information Security Technical Report, 14*(4), 186–196. https://doi.org/10.1016/j.istr.2010.04.004

COM/2022/454 final. (2022). Proposal for a Directive of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act). Retrieved March 25, 2024, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

COM/2022/495 final. (2022). Proposal for a Directive of the European Parliament and of the Council on liability for defective products (New Product Liability Directive). Retrieved March 25, 2024, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0495

Preliminary post incident review (pir): Content configuration update impacting the falcon sensor and the windows operating system (bsod). Retrieved July 24, 2024, from https://www.crowdstrike.com/falcon-contentupdate-remediation-and-guidance-hub/

CVE-2016-2148. (2016) Heap-based buffer overflow in the DHCP client (udhcpc) in BusyBox before 1.25.0 allows remote attackers to have unspecified impact via vectors involving OPTION_6RD parsing. Retrieved March 25, 2024, from https://www.cvedetails.com/cve/CVE-2016-2148/

CVE-2018-1000517. (2018). BusyBox project BusyBox wget version prior to commit 8e... contains a buffer overflow vulnerability. Retrieved March 25, 2024, from https://www.cvedetails.com/cve/CVE-2018-1000517/

CVE-2022-48174. (2022). There is a stack overflow vulnerability in ash.c:6030 in BusyBox before 1.35. Retrieved March 25, 2024, from https://www.cvedetails.com/cve/CVE-2022-48174/

Cybersecurity & Infrastructure Security Agency. (2024). Industrial Control Systems. Retrieved March 25, 2024, from https://www.cisa.gov/topics/industrial-control-systems

Cybersecurityhelp. (2022). #U65004 OS command injection in BusyBox. Retrieved from https://www.cybersecurity-help.cz/vulnerabilities/65004/

Dailymail, (2016). Cyber attacks cripple Twitter, Netflix, other websites. Retrieved March 25, 2024, from http://www.dailymail.co.uk/wires/afp/article-3859624/Twitter-Spotify-websites-shut-DDOS-attack.html

Dibia, V., & Wagner, C. (2015). Success within app distribution platforms: the contribution of app diversity and app cohesivity. (4304–4313) https://doi.org/10.1109/HICSS.2015.515

Directive (EU) 2022/2555. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Retrieved March 25, 2024, from http://data.europa.eu/eli/dir/2022/2555/oj

Economides, N., & Katsamakas, E. (2006). Two-sided competition of proprietary vs. open source technology platforms and the implications for the software industry. *Management Science*, *52*(7), 1057–1071 https://doi.org/10.1287/mnsc.1060.0549

Eden, P., Blyth, A., Jones, K., Soulsby, H., Burnap, P., Cherdantseva, Y., & Stoddart, K. (2017). SCADA System Forensic Analysis Within IIoT. In: Advanced Manufacturing, Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing (pp. 73–101). Springer.

Eltayeb, M.A. (2017). Internet of Things: Privacy and security implications. *International Journal of Hyperconnectivity and the Internet of Things*, *1*(1), https://doi.org/10.4018/IJHIoT.2017010101

Faber, B., & Günther, O. (2007). Distributed ONS and its impact on privacy. *IEEE International Conference on Communications*, (1223–1228) https://doi.org/10.1109/ICC.2007.207

Fabozzi, F. J., Kolm, P. N., Pachamanova, D. A., & Focardi, S. M. (2007). *Robust portfolio optimization and management*. John Wiley.

Facin, A. L. F., de Vasconcelos Gomes, L. A., de Mesquita Spinola, M., & Salerno, M. S. (2016). The evolution of the platform concept: a systematic review. *IEEE Transactions on Engineering Management, 63*(4), 475–488. https://doi.org/10.1109/TEM.2016.2593604

Federal Trade Commission. (2017). FTC charges D-Link put consumers' privacy at risk due to the inadequate security of its computer routers and cameras: Device-maker's alleged failures to reasonably secure software created malware risks and other vulnerabilities. Retrieved March 25, 2024, from https://www.ftc.gov/news-events/news/press-releases/2017/01/ftc-charges-

d-link-put-consumers-privacy-risk-due-inadequate-security-its-computer-routers-cameras

Fichman, R. G. (2014). Real options and IT platform adoption: implications for theory and practice. *Information Systems Research, 15*(2), 132–154. https://doi.org/10.1287/isre.1040.0021

Financial Times (2024). Companies around the world hit by Microsoft outage. Retrieved July 19, 2024, fromhttps://www.ft.com/content/fba9b61d-efcf-4348-b640-ccb1f9d18ced

Frank, M., Jaeger, L., & Ranft, L. M. (2022). Contextual drivers of employees' phishing susceptibility: Insights from a field study. *Decision Support Systems, 160*, 113818. https://doi.org/10.1016/j.dss.2022.113818

Gawer, A. (2014). Bridging differing perspectives on technological platforms: toward an integrative framework. *Research Policy, 43*(7), 1239–1249. https://doi.org/10.1016/j.respol.2014.03.006

Gepp, M., Foehr, M., & Vollmar, J. (2016). Standardization, modularization and platform approaches in the engineer-to-order business – review and outlook. In: Proceedings of the Annual IEEE Systems Conference. https://doi.org/10.1109/SYSCON.2016.7490549

Giesecke, K. (2004). Credit risk modeling and valuation: an introduction. *Credit Risk: Models and Management,2*,. https://doi.org/10.2139/ssrn.479323

Giesecke, K., & Weber, S. (2004). Cyclical correlations, credit contagion, and portfolio losses. *Journal of Banking and Finance, 28*(12), 3009–3036. https://doi.org/10.1016/j.jbankfin.2003.11.002

Hampson, M. (2019) IoT security risks: drones, vibrators, and kids' toys are still vulnerable to hacking. Retrieved March 25, 2024, from https://spectrum.ieee.org/iot-security-risks-drones-vibrators-iot-devices-kids-toys-vulnerable-to-hacking

Hartwich, E., Rieger, A., Sedlmeir, J., Jurek, D., & Fridgen, G. (2023). Machine economies. *Electronic Markets,33*,. https://doi.org/10.1007/s12525-023-00649-0

Helbing, D. (2013). Globally networked risks and how to respond. *Nature, 497*(7447), 51–59. https://doi.org/10.1038/nature12047

Howard, J.D., & Longstaff, T.A. (1998). *A common language for computer security incidents*. Sandia National Laboratories

Huber, R.X.R., Lockl, J., Röglinger, M., & Weidlich, R., (2024). The Concept of a Smart Action–Results from Analyzing Information Systems Literature. *Communications of the Association for Information Systems*, *54*(1), 6 https://doi.org/10.17705/1CAIS.05408

ICS-CERT. (2018a). ICSA-15-260-01: Harman-Kardon Uconnect vulnerability. Retrieved March 25, 2024, from https://ics-cert.us-cert.gov/advisories/ICSA-15-260-01

ICS-CERT. (2018b). ICSA-17-208-01: Continental AG Infineon S-Gold 2 (PMB 8876). Retrieved March 25, 2024, from https://ics-cert.us-cert.gov/advisories/ICSA-17-208-01

ISO/SAE 21434:2021. (2021). Road vehicles: Cybersecurity engineering standard of the International Organization for Standardization. Retrieved March 25, 2024, https://www.iso.org/standard/70918.html

Kang, C. M., Hong, Y. S., Huh, W. T., & Kang, W. (2015). Risk propagation through a platform: the failure risk perspective on platform sharing. *IEEE Transactions on Engineering Management, 62*(3), 372–383. https://doi.org/10.1109/TEM.2015.2427844

Karale, A. (2021). The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. *Internet of Things,15*,. https://doi.org/10.1016/j.iot.2021.100420

Keoh, S. L., Kumar, S. S., & Tschofenig, H. (2014). Securing the Internet of Things: A standardization perspective. *IEEE Internet of Things Journal, 1*(3), 265–275. https://doi.org/10.1109/JIOT.2014.2323395

Kim, K., & Altmann, J. (2020). Platform provider roles in innovation in software service ecosystems. *IEEE Transactions on Engineering Management, 69*(4), 930–939. https://doi.org/10.1109/TEM.2019.2949023

Kocher, P., Horn, J., Fogh, A., Genkin, D., Gruss, D., Haas, W.,..., Yarom, Y. (2018). Spectre attacks: Exploiting speculative execution. Retrieved March 25, 2024, https://spectreattack.com/spectre.pdf

Kim, D.-h., Lee, H., Kwak, J. (2017). Standards as a driving force that influences emerging technological trajectories in the converging world of the internet and things: An investigation of the M2M/IoT patent network. *Research Policy, 46*(7), 1234–1254. https://doi.org/10.1016/j.respol.2017.05.008

Lee, C. H., Geng, X., & Raghunathan, S. (2016). Mandatory standards and organizational information security. *Information Systems Research., 27*(1), 70–86. https://doi.org/10.1287/isre.2015.0607

Lemos, R. (2024). SAST, DAST, IAST, and RASP: Pros, cons and how to choose. Techbeacon. Retrieved March 25, 2024, from https://techbeacon.com/sast-dast-iast-rasp-pros-cons-how-choose

Li, S., Xu, L. D., & Zhao, S. (2015). The Internet of Things: A survey. *Information Systems Frontiers, 17*(2), 243–259. https://doi.org/10.1007/s10796-014-9492-7

Lins, M., Mayrhofer, R., Roland, M., Hofer, D., & Schwaighofer, M. (2024). On the critical path to implant backdoors and the effectiveness of potential mitigation techniques: Early learnings from xz. https://doi.org/10.48550/arXiv.2404 08987

Linton, M., & Parseghian, P. (2018). Today's CPU vulnerability: What you need to know. Retrieved March 25, 2024, from https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html

Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, W., Fogh, A., ..., Hamburg, M. (2018). Meltdown. Retrieved March 25, 2024, from https://meltdownattack.com/meltdown.pdf

Medeiros, J. (2017). WannaCry laid bare the NHS' outdated IT network – and it's still causing problems: The effects of the WannaCry attack are still being felt at NHS hospitals. Retrieved July 25, 2024, from http://www.wired.co.uk/article/nhs-cyberattack-it-ransomware

Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journal, 6*(5), 8182–8201. https://doi.org/10.1109/JIOT.2019.2935189

Meredith, J. R., Raturi, A., Amoako-Gympah, K., & Kaplan, B. (1989). Alternative research paradigms in operations. *Journal of Operations Management, 8*(4), 297–326. https://doi.org/10.1016/0272-6963(89)90033-8

Microsoft Threat Intelligence. (2021). Guidance for preventing, detecting, and hunting for exploitation of the Log4j 2 vulnerability. Retrieved March 25, 2024, from https://www.microsoft.com/en-us/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/#attacks

Miller, B., & Rowe, D. (2012). A survey SCADA of and critical infrastructure incidents. *1st Annual Conference on Research in Information Technology*, 51–56 https://doi.org/10.1145/2380790.2380805

Ministry of Internal Affairs and Communications, National Institute of Information and Communications Technology. (2019). The "NOTICE" project to survey IoT devices and to alert users. Retrieved March 25, 2024, from https://www.nict.go.jp/en/press/2019/02/01-1.html

Mohamad Noor, M., & Haslina Hassan, W. (2019). Current research on Internet of Things (IoT) security: a survey. *Computer Networks, 148*(15), 283–294. https://doi.org/10.1016/j.comnet.2018.11.025

Neville-Neil, G. V. (2017). IoT: The Internet of Terror. *Communications of the ACM, 60*(10), 46–37. https://doi.org/10.1145/3132728

Nicolescu, R., Huth, M., Radanliev, P., & Roure, D. D. (2018). Mapping the values of IoT. *Journal of Information Technology, 33*(4), 345–360. https://doi.org/10.1057/s41265-018-0054-1

Porch, C., Timbrell, G., & Rosemann, M. (2015). Platforms: a systematic review of the literature using algorithmic histography. https://doi.org/10.18151/7217443

Prakash, B. A., Chakrabarti, D., Valler, N. C., Faloutsos, M., & Faloutsos, C. (2012). Threshold conditions for arbitrary cascade models on arbitrary networks. *Knowledge and Information Systems, 33*(3), 549–575. https://doi.org/10.1007/s10115-012-0520-y

Püschel, L., Schlott, H., & Röglinger, M. (2016). What's in a smart thing? Development of a multi-layer taxonomy. *Proceedings of the 37th International Conference on Information Systems*. Retrieved March 25, 2024, from https://aisel.aisnet.org/icis2016/DigitalInnovation/Presentations/6

Radanliev, P., Roure, D. C. D., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., & Burnap, P. (2018). Future developments in cyber risk assessment for the Internet of Things. *Computers in Industry, 102*, 14–22. https://doi.org/10.1016/j.compind.2018.08.002

Rainer, R. K., Jr., Snyder, C. A., & Carr, H. H. (1991). Risk analysis for information technology. *Journal of Management Information Systems, 8*(1), 129–147. https://doi.org/10.1080/07421222.1991.11517914

Ransbotham, S., Fichman, R. G., Gopal, R., & Gupta, A. (2016). Special section introduction - ubiquitous IT and digital vulnerabilities. *Information System Research, 27*(4), 834–847. https://doi.org/10.1287/isre.2016.0683

Rausand, M., Barros, A., & Hoyland, A. (2020). System Reliability Theory: Models, Statistical Methods, and Applications. John Wiley & Sons. https://doi.org/10.1002/9781119373940

Regulation (EU) 2016/679. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved March 25, 2024, from http://data.europa.eu/eli/reg/2016/679/oj

Regulation (EU) 2018/858. (2018). Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC. Retrieved March 25, 2024, from http://data.europa.eu/eli/reg/2018/858/oj

Regulation (EU) 2019/2144. (2019). Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166. Retrieved March 25, 2024, from http://data.europa.eu/eli/reg/2019/2144/oj

Rieger, A., Thummert, R., Fridgen, G., Kahlen, M., & Ketter, W. (2016). Estimating the benefits of cooperation in a residential microgrid: A data-driven approach. *Applied Energy, 180*, 130–141. https://doi.org/10.1016/j.apenergy.2016.07.105

Ronen, E., O'Flynn, C., Shamir, A., & Weingarten, A.O. (2016). IoT goes nuclear: creating a ZigBee chain reaction. Retrieved March 25, 2024, from https://eprint.iacr.org/2016/1047.pdf

Roy, A. D. (1952). Safety first and the holding of assets. *Econometrica, 20*(3), 431. https://doi.org/10.2307/1907413

Sadeghi, A.R., Wachsmann, C., & Waidner, M. (2015). Security and privacy challenges in industrial Internet of Things. *Proceedings of the 52nd Annual Design Automation Conference*. https://doi.org/10.1145/2744769.2747942

Sicari, S., Cappiello, C., Pellegrini, F. D., Miorandi, D., & Coen-Porisini, A. (2016). A security-and quality-aware system architecture for Internet of Things. *Information Systems Research, 18*(4), 665–677. https://doi.org/10.1007/s10796-014-9538-x

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM SIGMIS Database, 38*(1), 60–80. https://doi.org/10.1145/1216218.1216224

Slaughter, S. A., Harter, D. E., & Krishnan, M. S. (1998). Evaluating the cost of software quality. *Communications of the ACM, 41*(8), 67–73. https://doi.org/10.1145/280324.280335

Smartfrog Ltd. (2012). Open source terms. Retrieved March 25, 2024, from https://www.smartfrog.com/en-us/open-source-terms

Syed, R. (2020). Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system. *Information & Management, 57*(6), 103334. https://doi.org/10.1016/j.im.2020.103334

Temizkan, O., Park, S., & Saydam, C. (2017). Software diversity for improved network security: Optimal distribution of software-based shared vulnerabilities. *Information Systems Research, 28*(4), 828–849. https://doi.org/10.1287/isre.2017.0722

Thielmann, S. (2017). Acting federal trade commission head: Internet of Things should self-regulate. Retrieved March 25, 2024, from https://www.theguardian.com/technology/2017/mar/14/federal-trade-commission-internet-things-regulation

Thomas, L. D. W., Autio, E., & Gann, D. M. (2014). Architectural leverage: Putting platforms in context. *Academy of Management Perspectives, 28*(2), 198–219. https://doi.org/10.5465/amp.2011.0105

TomTom, T. (2005). Open source software: TomTom GO 4. Retrieved March 25, 2024, from https://www.tomtom.com/de_at/opensource/go-version-4

Travis, G. (2019). How the Boeing 737 Max disaster looks to a software developer. *IEEE Spectrum*, *18*. Retrieved from https://spectrum.ieee.org/how-the-boeing-737-max-disaster-looks-to-a-software-developer

Vermesan, O., & Friess, P. (Eds.) (2022). Digitising the industry Internet of Things connecting the physical, digital and VirtualWorlds. Taylor & Francis

Violino, B. (2017). FTC vs D-Link: The legal risks of IoT insecurity: Vulnerabilities in connected devices spell potential trouble for product manufacturers. Retrieved March 25, 2024, from https://www.zdnet.com/article/ftc-vs-d-link-the-legal-risks-of-iot-insecurity/

Vectra AI Security Research Team. (2016). How a webcam Can Be exploited as a backdoor, 2024-07-25. https://www.vectra.ai/blog/turning-a-webcam-into-a-backdoor

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Waldo, J. (2002). Virtual organizations, pervasive computing, and an infrastructure for networking at the edge. *Information Systems Frontiers, 4*(1), 9–18. https://doi.org/10.1023/A:1015322219248

Walters, R., & Jordan, J. (2016). US must remain vigilant to counter cyberattacks. Retrieved March 25, 2024, from http://dailysignal.com/2016/10/26/how-a-cyberattack-took-down-twitter-netflix-and-the-new-york-times/

Wang, H., He, H., Zhang, W., Liu, W., Liu, P., & Javadpour, A. (2022). Using honeypots to model botnet attacks on the Internet of Medi-

cal Things. *Computers and Electrical Engineering, 102*, 108212. https://doi.org/10.1016/j.compeleceng.2022.108212
Watts, D.J. (2002). In *A simple model of global cascades on random networks* (Vol. 99, 5766–5771). https://doi.org/10.1073/pnas.082090499
Weber, R. H. (2010). Internet of Things - new security and privacy challenges. *Computer Law & Security Review, 26*(1), 23–30. https://doi.org/10.1016/j.clsr.2009.11.008
Weber, R. H. (2013). Internet of Things - governance quo vadis? *Computer Law & Security Review, 29*(4), 341–347. https://doi.org/10.1016/j.clsr.2013.05.010
Weigl, L., Barberea, T., Sedlmeir, J., & Zavolokina, L. (2023). Mediating the tension between data sharing and privacy: The case of DMA and GDPR. In: Proceedings of the 31st European Conference on Information Systems, AIS. Retrieved from https://aisel.aisnet.org/ecis2023_rip/49/
West, J. (2003). How open is open enough? Melding proprietary and open source platform strategies. *Research Policy, 32*(7), 1259–1285. https://doi.org/10.1016/S0048-7333(03)00052-0
Whitmore, A., Agarwal, A., & Xu, L. D. (2015). The Internet of Things - a survey of topics and trends. *Information Systems Frontiers, 17*(2), 261–274. https://doi.org/10.1007/s10796-014-9489-2
Yoo, Y. (2010). Computing in every day life: A call for research on experiential computing. *MIS Quarterly, 34*(2), 213–231. https://doi.org/10.2307/20721425
Yoo, Y., Jr., R. J. B., Lyytinen, K., & Majchrzak, A. (2012). Organizing for innovation in the digitized world. *Organization Science, 23*(5), 1398–1408. https://doi.org/10.1287/orsc.1120.0771
York, D. (2018). Meltdown and Spectre: Why we need vigilance, upgradeability, and collaborative security. Retrieved March 25, 2024, from https://www.internetsociety.org/blog/2018/01/meltdown-spectre-need-vigilance-upgradeability-collaborative-security/
Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2019). The effect of IoT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved. *Internet of Things Journal, 6*(2), 1606–1616. https://doi.org/10.1109/JIOT.2018.2847733

Martin Brennecke is a doctoral researcher at the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg. In his research, he investigates the impact of digital infrastructure decentralization on individuals, organizations, and society. He holds a master's degree in international economics and governance, as well as a bachelor's degree in philosophy and economics.

Gilbert Fridgen is a full professor and PayPal FNR PEARL Chair in Digital Financial Services at the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, and coordinator of the National Centre of Excellence in Research on Financial Technologies (NCER-FT). In his research, he analyzes the transformative effects of digital technologies on individual organizations and on the relationship between organizations. He addresses especially emerging technologies like distributed ledgers, digital identities, machine learning, and the internet of things.

Jan Jöhnk is a product owner at the commercial insurance company HDI Global SE in Hanover, Germany, and an affiliated researcher at the FIM Research Institute for Information Management. He received his doctorate in Information Systems and Strategic IT Management from the University of Bayreuth and visited the Department of Digitalization at Copenhagen Business School for a research stay. In his research, Jan is especially interested in questions of digital transformation at the interface of IT organization, IT management, and emerging technologies.

Sven Radszuwill is a department head for new products and services at a health-tech software company, former researcher at the University of Bayreuth and Fraunhofer FIT in the area of digital networks, project management, and distributed ledger technologies.

Johannes Sedlmeir is a postdoctoral researcher at the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg. In his research, he focuses on the effective use of emerging digital technologies in organizations by designing and evaluating innovative IT artifacts based on, e.g., distributed ledgers, digital identity attestations, and zero-knowledge proofs.