Investigating System Operators' Perspective on Security Misconfigurations

Constanze Dietrich
Berliner Hochschule für Technik*
constanze.die@gmail.com

Katharina Krombholz
CISPA Helmholtz Center (i.G.)†
krombholz@cispa.saarland

Kevin Borgolte
UC Santa Barbara
kevinbo@cs.ucsb.edu

Tobias Fiebig
TU Delft
t.fiebig@tudelft.nl

ABSTRACT

Nowadays, security incidents have become a familiar "nuisance," and they regularly lead to the exposure of private and sensitive data. The root causes for such incidents are rarely complex attacks. Instead, the attacks are straight-forward, and they are enabled by simple misconfigurations, such as authentication not being required, or security updates not being installed. For example, the leak of over 140 million Americans' private data from Equifax's systems ranks among most severe misconfigurations in recent history: The underlying vulnerability was long known, and a security patch had been readily available for months, but it was never applied. Ultimately, Equifax blamed an employee for forgetting to update the affected system, highlighting the *personal* responsibility of that operator.

In this paper, we investigate the operators' perspective on security misconfigurations to approach the human component of this class of security issues. We focus our analysis on system operators, as although they are the relevant *actors* managing the affected systems, they have not yet received significant attention by prior research. We follow an inductive approach and apply a multi-step empirical methodology: *(i)* a *qualitative* study to understand how to approach the target group and measure the misconfiguration phenomenon, and *(ii)* a *quantitative* survey rooted in the qualitative data. We then provide the first analysis of system operators' perspective on security misconfigurations, and we determine the factors that operators perceive as the root causes. Based on our findings, we provide practical recommendations on how to reduce security misconfigurations' frequency and impact.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**; Usability in security and privacy; • **Social and professional topics → Employment issues**; **Computing occupations**;

KEYWORDS

Computer systems; system operations; operators; administrators; security; misconfigurations; vulnerabilities; human factors.

ACM Reference Format:
Constanze Dietrich, Katharina Krombholz, Kevin Borgolte, and Tobias Fiebig. 2018. Investigating System Operators' Perspective on Security Misconfigurations. In *2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18), October 15–19, 2018, Toronto, ON, Canada.* ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3243734.3243794

CCS '18, October 15–19, 2018, Toronto, ON, Canada

1 INTRODUCTION

Security incidents and vulnerabilities in today's Internet are often believed to be caused by programming errors, such as faulty input validation, race conditions, or buffer overflows, that are exploited to disrupt services without the vulnerability being publicly known and before a patch is available (0 days). However, when investigating recent security incidents, such as those of Equifax [2, 3], we find a different picture. The vulnerability exploited in the primary Equifax incident, in which personally identifiable information of 143 million customers were inadvertently disclosed and which sparked a congressional inquiry, was clearly a programming mistake. However, while a patch to address the bug was released months prior, it was simply not yet deployed to the production environment.

Of course, not applying (security) patches can have its cause in countless reasons, such as technical debt accumulated over time, or availability and functionality requirements. Yet, when investigating the Equifax incident, such complex reasons are not the breach's cause. In the end, Equifax blamed the entire incident on a single operator for forgetting to install security patches in time [4].

Broadening the scope, incidents that have their root cause in human error can be found all over the Internet, from basic infrastructure to applications [5, 6]. For example, in early 2015, over 40,000 MongoDB instances were publicly accessible from the Internet, without authentication and authorization, and, in turn, allowed anyone to retrieve the stored data [7], which might have been confidential or possibly would have even required governmental security clearances. In fact, one of these MongoDB instances contained millions of voting records from Mexican citizens, and, in turn, it leaked them online [8]. Other database systems, like Redis or memcached, are not spared from similar human error: hundreds of thousands of systems were discovered to be unprotected [6]. The configuration of Transport Layer Security (TLS) for web application servers are often similarly vulnerable to misconfigurations due to human error [9]. Ultimately, misconfigurations can also lead to other vulnerabilities, such as servers becoming vulnerable to denial-of-service attacks [10, 11], or websites turning malicious [12] or being defaced to embarrass the systems' operators [13, 14].

The overarching aspect of these incidents is that the mistake leading to the incident occurred during the *operation* of the affected system instead of its *development* (as it is the case for software vulnerabilities). These mistakes do not need to be complex, but they can even be comparatively simple errors, such as missing or incorrect

*We use "Berliner Hochschule für Technik" instead of "Beuth Hochschule für Technik Berlin" because of Peter Christian Wilhelm Beuth's antisemitic views [1]. We stand for a diverse and inclusive scientific community, and we do not want to perpetuate the name of a researcher who did not.

†Research partially performed while at SBA Research.

firewall rules, faulty or missing authentication, or software dependencies, for which security updates were not installed. Following, we use *misconfiguration* as the covering term for such (human) errors in the operation of systems, and we use *security misconfiguration* when such an error allows an attacker to impact the confidentiality, integrity, or availability of a system (i.e., its security). The corresponding actors are called *operators* (also called administrators, or admins, sometimes prefixed with the type of system that they operate, for example, network operator or system administrator), and they are responsible for configuring systems to fit them to an organization's specific needs.

In this paper, we investigate the operators' perspective on security misconfigurations. Specifically, we aim to answer the following questions:

(1) Do security misconfigurations (regularly) occur in practice?
(2) If security misconfigurations occur commonly, what are the reasons as to why they occur?
(3) Do security misconfigurations lead to security incidents?
(4) If security misconfigurations led to security incidents, were the misconfigurations known and addressable?
(5) If security misconfigurations were known and could have been addressed, what caused them not to be addressed?

To do so, we use a multi-step empirical approach, first approaching the target group with a qualitative study to lay the foundation for a subsequent quantitative evaluation. We investigate the subject matter in an explorative, open-minded way, to elicit a picture on operators' perceptions, without being biased by seemingly established concepts and beliefs within the *research community*. Hence, we contribute the first empirical analysis from the operators' perspective, collecting a data set that can serve as the foundation and point for comparison in future work.

We make the following major contributions:

- We present the first qualitative and quantitative study that investigates operators' perceptions of factors leading to security misconfigurations.
- Our results indicate that the majority of security misconfigurations have not (yet) led to security incidents, which suggests that countless undiscovered issues may be present in Internet-connected systems.
- We identify social (communication), structural, and, institutional factors to be major facilitators for bad security posture based on our analysis of the operators' perspectives on misconfiguration facilitators.
- We find that structural and procedural mitigations already exist that would prevent most security misconfigurations that our participants encountered, but that these procedures are often not in place for various reasons.
- We provide practical recommendations on how to reduce and the frequency and impact of security misconfigurations.

Outline. First, we describe our ethical considerations (Section 2). Next, we detail the methodology of our qualitative approach (Section 3), which is followed by our qualitative results (Section 4). We then discuss the methodology of our quantitative study (Section 5) and analyze the collected quantitative data (Section 6). Finally, we compare to related work (Section 7), discuss the limitations of our work (Section 8), and summarize our key findings (Section 9).

2 ETHICAL CONSIDERATIONS

For the research of this paper, we conducted interviews and surveys that involve human subjects, and we collected data about their experience. Furthermore, our subjects might be inclined to talk about past behavior. As such, the nature of our research renders it inherently challenging yet critically important to execute it ethically. At the time the research was conducted none of the then relevant host institutions had an Institutional Review Board (IRB) or a similar committee advising on potential ethical issues. Hence, we independently followed the guidelines set out by the Menlo Report by the U.S. Department of Homeland Security [15, 16].

The participants of both studies were informed about the purpose of the studies and gave their consent to using the data for research purposes. For the interviews, participants had the option to review and redact the transcripts for confidential information before we entered them into our research pipeline (including anonymization) and they were also allowed to opt out and withdraw from our study at any point. Particularly the option to redact and withdraw from the study is crucial because pre-studies indicated that participants may be overly cautious if these options are not provided, due to being concerned about accidentally violating non-disclosure agreements or private data. We did not question or deny any requests for redaction, and we did not require any justification.

To preserve the anonymity of participants, we anonymized all items that constitute Personally Identifiable Information (PII) prior to analyzing the data. Furthermore, given that we are analyzing responses of individuals online, we consider their aliases/nicknames as PII. Correspondingly, for our quantitative study, we collected minimal PII in aggregated form only (e.g., a participant's age was collected in range bins), and we did not collect other PII at all, such as gender, nationality, etc. Instead, we focused our survey on professional information of the subjects, while ensuring that this information cannot reveal the participants' identities.

3 QUALITATIVE METHODOLOGY

The literary body on misconfigurations and their security impact is still sparse, which is why we followed an inductive approach [17] and used a qualitative study as a starting point for our quantitative study. Following, we detail our study design, recruitment procedure, and target population.

3.1 Interview Study Design

To better assess the respondents' perceptions and opinions on security misconfigurations, we opted for semi-structured interviews with specific, yet open-ended questions. Our goal is to get a broader overview of systemic influences by letting participants digress when answering, which might happen because operators tend to be enthusiastic about their work (judging from our initial experience).

We started each interview with a brief introduction of ourselves, the study, and its research goals. Furthermore, we encouraged participants to provide technical and in-depth explanations of operations related topics. Subsequently, we engaged in three preset questions, which we selected based on the initial encounter:

(1) **Which security-related misconfigurations have you encountered?**
This question aims to investigate the types of misconfigurations that can emerge during operations, and the systems

that might be misconfigured easily or often. We also asked *how* the interviewee discovered the mistakes, to understand what reveals security misconfigurations. We then inquired whether the security misconfigurations led to security incidents, and how they think that the misconfigurations could have been prevented.

(2) **How do you think misconfigurations occurred?** This question allows operators to conjecture on possible factors that facilitate misconfigurations. We did not restrict answers to specific incidents, and also allow participants to include *perceived* factors.

(3) **How did misconfigurations affect you and the way your company approaches and handles security?** This question aims at understanding if the personal work attitude or habits have changed in response to a security misconfiguration, or if there were sanctions or changes in configuration procedure after an incident took place.

3.2 Data Analysis

To analyze the interviews, we collected anonymized Internet Relay Chat (IRC) log files. In a first round, we analyze the anonymized interviews with QDA Miner [18], and gradually generate categories while keeping the underlying codes rather specific to not generalize them prematurely. Subsequently, we perform inductive coding [19–24], which is commonly used to construct models and theories based on qualitative data in social sciences and usable security [9, 25].

We then use Strauss and Corbin's descriptive, axial coding [23] and selective coding to group our data into categories and models. We first code, then iteratively refine our research questions, with an emphasis on the different stages of coding.

We use one coder to construct the code book, which is deemed acceptable in social sciences, especially when the analysis is interpretative and exploratory [26]. An additional researcher, who had not been involved in the data collection, then uses the codebook to assess the frequency of codes in the interviews. We pay special attention to cases in which the participants exhibit strong opinions, which appear to be the most challenging tasks, and how they explain misconfiguration facilitators in conjunction with the underlying root causes. Due to our community-driven approach (Section 3.3), most interviews were in German. These interviews are analyzed by a German native speaker. We pay special attention to preserve meaning, tone, and, context when translating them into English. In the case of English-speaking participants, we do *not* correct typographical or grammatical mistakes.

3.3 Operators as a Target Group

Operators are personnel who are tasked with configuring and maintaining complex systems. Therefore, they constitute an ideal starting point for an investigation of multi-domain causes for security misconfigurations. However, operators are, like developers [27], a vocationally enclosed group, or as Halprin phrased it: *"The average system administrator's day consists of so many complimentary and contradictory tasks that they often find it difficult to describe to other people what it is that they do."* [28]. Furthermore, they perform *"[…] such a wide variety of tasks each and every day, that it is often difficult to remember what they did before lunch."* [28]. Even though Halprin's observations stem from 1998, they remain valid today. In general, operators tend to be highly restricted in their time commitments [29]. Therefore, any additional tasks, such as participating in a research study, must be sufficiently incentivized. Unfortunately, traditional recruitment methods, that is, monetary incentives, are not applicable: Operators are generally well compensated and more concerned about committing their time than receiving additional pay [29]. Correspondingly, we did not compensate interviewees.

Additionally, typical recruitment strategies, such as (mass) mailing campaigns, are also problematic: Operators are skeptical about unsolicited mail, due to being regularly confronted with spam and phishing at work [30]. Furthermore, there is no central database of system operators' contact addresses that could be used to launch a campaign for recruitment, contrary to, for example, Android Developers [31]. Therefore, we opted for a community-driven approach to contact the target population.

Recruitment. In the context of our study, the operators are domain experts. However, the topic of our study bears a primarily negative connotation and operators might be embarrassed to admit misconfigurations. To address this problem, we aimed to create a safe environment in which they felt comfortable to disclose misconfigurations, also knowing that their data was treated confidentially. During our initial engagement, several operators expressed that the best place to recruit participants would be via IRC.

We used the channel of the German Network Operators Group (DENOG) to recruit participants, which means that the operators of our study are members of an online community. Note that, for a lot of operators, IRC is usually running in the background ("idling") and used to share news and ask specific questions. Similarly, operators seek leisure time in IRC, discussing various topics with people in their community. Therefore, in conjunction with earlier observations on time pressure and commitments, we framed our interview about misconfigurations as a way to find leisure and to relax. Overall, we conducted interviews with 6 participants online via IRC for our qualitative study, which did not reach theoretical saturation [32]. However, the potential lack of saturation is alleviated as our qualitative analysis is only used as a first step for our quantitative study. Additionally, the target population is diverse with respect to different (demographic) aspects, such as their relationship to the organization ranging from freelancer consulting for companies of various sizes to administrators from non-governmental organizations (NGO) to medium to large organizations. Furthermore, administrators are diverse with respect to their role within a team (e.g., team lead, administrator, engineer, or consultant) and their education and previous work experience.

4 QUALITATIVE RESULTS

In this section, we discuss the results from our qualitative evaluation. For eased readability, we use pseudonyms for all participants instead of IDs. Following, we group the results of our *qualitative* research steps into six major categories (Table 2), from which we derive theories that we test through our subsequent quantitative investigation.

4.1 Background and Demographics

Due to the nature of our target group and the focus on their perceptions of misconfigurations, we did not *request* in-depth information about the participants' employers. Especially in the context of

Pseudonym	Background	Language
Alex	Former database administrator (DBA), now DBA team lead, large organization, mostly databases and Red Hat Linux	German
Benjamin	Operator focusing on networking/systems, organization size unclear	German
Christian	Linux administrator with additional networking tasks, medium-sized organization	German
David	Consultant, freelancer, mixed setup as used by the customers, not administrating himself anymore	German
Eno	Network operator, organization size unclear, also active in an NGO	German
Konstantin	Network engineer, large public healthcare provider	English

Table 1: Interview partners and their backgrounds

Category	Description
Misconfiguration Types	The technical misconfiguration and resulting security flaw
Impact of Security Incidents	Consequences for organizations, clients, and users
Misconfiguration Facilitating Factors	Why misconfigurations occurred
Impact on Work Environment	How an incident impacted the work environment
Detection	Circumstances leading to misconfiguration detection
Possible Mitigations	Methods, tools, and processes that *would* have prevented misconfigurations

Table 2: Coding-categories that emerged from interviews

Category	Example
Authentication	Faulty or missing identity verification
Passwords	Bad or publicly known (e.g., default) passwords
Updates	Missing or delayed (security-related) updates
Firewalls	Disabled firewalls, faulty filter settings
Encryption	Unencrypted login pages, bad SSL/TLS settings
Scripting	Faulty automation stalling system components
Storage	Backups on the same drive as the productive system
No hardening	Not following best current practices, although it has no *direct* security impact
Authorization	Faulty assignment of access privileges
Deployment	Publishing information like extended log files or version information in connect banners
Integration	Insufficiently separated systems (e.g., Internet and intranet), not adapting old configuration to new systems

Table 3: Misconfiguration types of the qualitative study

interviews, where participants may digress around questions, specific inquiries might have influenced their openness. Nonetheless, we include general information on their background, such as relative organization size or industry sector. We carefully examined the operators' statements about their *general* work environment to ensure that the participants did not accidentally reveal identifying information, and to redact such information before proceeding with the interviews. We also inquired about the operators' background, for example, which kind of systems they commonly operate. Our participants have diverse backgrounds (Table 1), spanning smaller and larger organizations as well as different aspects of operations, including networks, systems, and, (database) applications. Interestingly, as to why misconfigurations occur, the participants described their perceived issues in general, and regularly and explicitly noted that their comments are independent of any specific organization.

4.2 Coding Categories

Misconfiguration Types. This category contains the cases that the operators considered a security misconfiguration. We categorize them in eleven sub-categories (Table 3), which are intentionally technical. Although including the nature of the misconfiguration (its root cause) could yield interesting categories, such as the usage of defaults due to being misled by conventions, or lack of updates due to abandoned components (e.g., if the initially responsible person left the organization), it ultimately leads to fuzzy results as misconfigurations often have several contributing causes. Hence, we detach the *technical* mistake from its cause. This approach is more suitable to identify both misconfiguration types and the involved components.

Impact of Security Misconfigurations. During our study, interviewees were mostly vague on the *impact* of security misconfigurations. In many cases, the impact follows directly from the type of misconfiguration, like when an operator does not configure authentication, then unauthorized parties will have access. However, if the (potential) impact does not directly follow from the misconfiguration itself, then it is often not clear whether there has been an accompanying *incident*. Furthermore, even if an incident occurs, then the incident may still not be attributable to a *single* misconfiguration.

Misconfiguration Facilitators. Identifying misconfiguration facilitators is one of the objectives of our study. The interviewees' perceptions on potential causes yield a multitude of unique codes in which the operators explain what keeps them and their peers from configuring systems correctly and securely. We encouraged the participants to cover all aspects of potential factors, which resulted in several mutually dependent codes. In turn, a clear distinction and separation between them is challenging. Based on our coding, we systematically group codes relating to misconfiguration facilitators by the responsibility domains of the actors:

Systems
: This category relates to the systems involved, for example, complex setups, software with bad defaults, or, complex and confusing interfaces.

Operators
: This category includes personal shortcomings of the operators, such as overconfidence or insufficient knowledge.

Organizational Environment
: This category relates to the operators' organizational environment, including management, or policy implementation.

Systems. Factors relating to the systems that the operators use are predominantly *usability* issues, as Krombholz et al. also discovered [9]. For instance, Alex remarks: *"If you are setting up a new system, you have to learn how it works first. But getting it working is usually more important than figuring out which switches are there, and which have to be flipped so the system is working and secure."* The issues in this group have *technical* solutions: Pervasive usability, better system management tools, and secure-by-default [33].

Operators. The operators are the main actors in systems' operation, and we group factors together under the *operators'* umbrella

that relate to them personally. During our interviews, the most frequently mentioned issues on the operators' side was a lack of knowledge, experience, or concern, but also simple blunders, or as David put it: *"typos happen."*

Focusing on knowledge and experience, Eno states that most new operators, just right out of school, are *"[...] still wet behind their ears regarding security."* Similarly, on the matter of misleading tutorials perpetuating insecure solutions, like `chmod -Rv 0777 ./`, Christian mentions that *"with enough experience you would never do something like that. But it's written on the Internet."* Interestingly, Acar et al. [31] reported similar behavior among programmers.

On a self-reflective note, Konstantin reports why he misconfigured a firewall, exposing countless internal hospital systems: *"As to why, well I was fairly right out of school, unexperienced, and my education did not even prepare me for something so complex."*

Organizational Environment. In our classification, the organizational environment includes actions by the organizations' management team, as well as other institutional and policy-driven *external* factors, like standards and regulations. Particularly important is that personal and systemic factors can be amplified by the environment. For example, Konstantin continues his prior comment: *"I had very little training, our manager was the 'figure it out yourself type'. Which was common back then :)"*

The participants also reported unreasonable budget constraints, an unreflected faith in external suppliers, and consultants leading to issues. David remarks on why automation and quality assurance as remedies to typos and blunders are not implemented by a multinational network provider: *"They use external consultants up to the team-lead level. These cost 1/4 of an engineer in Germany. Why should they care about implementing quality assurance or automation?"*

Interviewees often trace these issues back to management having little to no understanding about what exactly the operators' day-to-day responsibilities look like. Such as when Konstantin and multiple colleagues tried to communicate to their manager that a security misconfiguration related issue in their network was in dire need to be addressed, the manager *"[...] then claimed we where just after buying fancy hardware, and overdoing [exaggerating] the severity of the warned about issues."* This may tie in with more structural communication issues, or as David remarks: *"From a manager's point of view all technicians are the same. Why? Because no matter to whom he talks, he does not understand him."*

Factor Frequency. In our analysis, we find that external factors appear more frequent than systems or personal factors. The most common factors that we encounter are "unqualified leadership" and "financial decisions." Interestingly, insufficient knowledge and concern are mentioned frequently, but other systemic reasons, such as poor defaults or usability issues, are mentioned rarely.

Impact of Misconfigurations on Job Attitude. Over the course of our interviews, we frequently encounter codes indicating that security misconfigurations lead to *some* positive change in job attitude. Konstantin comments on actions taken after an incident: *"We adopted a clear naming standard for our firewall rules and interfaces [...] The hospital in question started segmenting up there [their] network."* Similarly, Benjamin remarks that *"processes were adjusted"*. However, he also notes that *"Timepressure is usually not fixed, because everything has to be fast."* Several interviewees report that while actions were taken in response to an incident, they did not include a general commitment to security, but they were incident-driven remediation of the specific issues. More generally, the differing statements can be summarized by Christian's remark: *"Either you are embarrassed by your mistake and learn from it, or you establish more funny processes and buy useless security stuff. In large shops it's usually the latter."*

Detection. Looking at how misconfigurations are discovered in practice, we identify three principal cases: *(i)* detection due to an incident, *(ii)* accidental detection, and *(iii)* detection during an audit. In our interviews, Christian reports an example of *(i)*, namely how he encountered a misconfigured system because it was unaccounted for, security patches were not installed, and, in turn, it was compromised: *"Or you're wondering why there still are worm-infested Windows machines on your network and only then realize that the print-server of $printing-system also uses windows. Of course not having been updated for years."* In contrast, Benjamin explains how he accidentally stumbled upon a misconfiguration, insufficiently protected file shares, by chance: *"Chance is, if you are searching for something on a file share and suddenly stumble onto something that should not be there."* He also reports that found misconfigurations during security audits. However, based on the interviews, we cannot determine a clear distinction between audits as a method for detecting misconfigurations versus them being a method to preventing them in the first place.

Possible Mitigations. We identify four clusters from the mitigation strategy codes: *(i)* personal measures, *(ii)* non-personal measures including organizational strategies, *(iii)* postmortem strategies, and *(iv)* social strategies. Generally, system operators are confident that existing tools and procedures could mitigate security misconfigurations *if* they were used. Furthermore, a technique that received particular attention across operators are "blameless postmortems". Blameless postmortems are important and effective because, as Benjamin puts it, *"[...] they are not about figuring out who's guilty, but instead about finding a sustainable solution for the problem."*

Personal Measures. The operators also commonly mention personal behavior and actions to reduce the occurrence of misconfigurations in the first place. On the more straight-forward side, they suggest to be *mindful* about one's tasks and to pay *attention*. Similarly, having enough *time* to actually be mindful, *planning* well before making changes, and having a clear *overview* and *understanding* of the system are aspects that operators see themselves to be responsible for. To ensure some of these personal best practices, *Eno* aims to make changes to systems he operates only between 8 AM and 2 PM. Furthermore, they frequently mention that it is imperative to have enough *fundamental knowledge* of the task at hand, as well as sufficient experience in system operations.

Non-personal Measures. Foreshadowed by the perceived reasons for security misconfigurations leaning toward non-personal issues, operators also have strong tendencies toward process driven mitigations. For example, operators frequently mention that they require *processes* that enable them to work without making mistakes. Similarly, operators are concerned about the lack of understanding by

their managers on how diverse the knowledge in IT is and what technicians require in terms of environment, tools, and support to work effectively and efficiently. In turn, they also perceive their job as being a *translator between management and IT*, and they indicate that there should be more IT professionals bridging the communication gap between IT and management. This highlights the importance of *communication*, particularly across departments, which is tightly connected to the suggested social strategies.

Post-Mortem and Social Strategies. It is common practice to conduct a *postmortem* analysis after any incident, with the goal of identifying *what* went wrong and *why*. The operators in our study strongly emphasize that a postmortem *must* be *blameless*. In a blameless postmortem, personal responsibility and accountability is detached from the what and why. Specifically, a blameless postmortem aims to prevent operators from omitting the truth to avoid punishment for mistakes, which could obscure or cover the actual underlying causes for the incident, such as a lack of automation or poor procedures that lead to security misconfigurations.

4.3 Summary

Overall, our qualitative study reveals perceptions on the many interdependent facets of security misconfigurations. Our interviewees have a broad range of experiences with security misconfigurations. Based on our interviews, security misconfigurations appear to be a common problem in the operations community. Although technical mitigation strategies exist, operators still perceive mitigation strategies as rarely or insufficiently implemented and they see the principal reasons for misconfigurations in the institutional and management domain. The operators also highlight that the discovery of a security misconfiguration or an incident due to a misconfiguration itself often has a positive effect on a company's security posture. However, this positive effect can only be temporary. Based on these observations, we focus our quantitative analysis on three core themes:

(1) **Security misconfigurations are more common than the reported security incidents indicate.**
Security misconfigurations do not always lead to large-scale security incidents. Hence, they may not have been publicly disclosed. Based on our qualitative research, we assume that misconfigurations are a regular occurrence and every operator has encountered them previously.

(2) **Security misconfiguration facilitators are largely based in the management and institutional domain.**
Most discussed misconfiguration facilitators pertain to decisions by management or institutional characteristics, such as insufficiently allotted time to complete tasks, underspecified, missing, or overly restrictive processes, as well as unreasonable budget constraints. These conditions appear to be caused by a lack of understanding or trust toward the operators.

(3) **Security misconfigurations that result in security incidents make management and operations (temporarily) more security-sensitive.**
Several interviewees stated that discovering security misconfigurations made them more cautious. Furthermore, as incidents also involve management, the negative impact of misconfigurations (eventually) will make management more appreciative of security and incident prevention, which, in turn, increases their willingness to invest in the security measures that prevent or reduce the impact of misconfigurations. Importantly, it only increases their willingness if we expect the cost of an incident to be higher than its preventive measures, which has become a reasonable assumption today due to the theft and value of private data, and governmental fines [34].

5 QUANTITATIVE METHODOLOGY

To investigate the observations from the qualitative study, we conducted a broader quantitative study. We implemented our questionnaire using Google Forms [35].

5.1 Questionnaire Structure and Sections

We specifically design our questionnaire so that it allows investigating the previously stated observations.[1] To address multiple categories of subjects gracefully, there are multiple paths through our questionnaire, primarily based on the subjects' current state of employment (Figure 1). See the full questionnaire in Appendix A.

At the start of our questionnaire, we inform participants about the purpose of our study, and we explain the applicable privacy considerations. We also inform the participants that completing the survey will take between 10 and 20 minutes, depending on how many of the qualitative questions they will answer. Participants were not compensated for participating in our survey.

Throughout our survey and wherever an estimation within a certain range was needed, we use unipolar and bipolar five-step Likert-type scales with balanced options that would be perceived as equally far apart from each other [36].

We focus our survey on: *Occupation, Job Environment, Daily Business, Past Misconfiguration Experience, Misconfiguration Facilitating Factors, Consequences, Opinions, and Demographics.*

Occupation. Operators may work in different organizational setups and constellations. In fact, during our qualitative study, some operators were working as independent consultants, other operators were employed by a company, and others again have left the profession, but remain involved in the operations community and still have important insights to share. To address these three groups correctly in wording and to classify their responses appropriately, our questionnaire is divided in *three branches* (Figure 1). Each branch uses the same structure and types of questions, but the wording is adjusted to fit the operator's employment situation (e.g., a consultant has customers, while an employed operator has managers).

Job Environment. We also investigate the institutional environment that the operators work in. This includes the operators' job titles, whether it matches what they are actually doing, and, if they perceive themselves as operators. Participants that did not consider themselves as operators are led to an exit page, and we thank them for their participation. We also ask about the organizations' size or industry for an in-depth analysis of the prevalence of misconfigurations in future work.

Daily Business. The next part of our survey deals with what our respondents do on a day-to-day basis, for example, what kind of IT systems they operate and how they would estimate their expertise in the respective fields. Furthermore, to assess working experience, we also record how long they have been operators.

[1] The questionnaire covers additional topics that are beyond the scope of this paper.

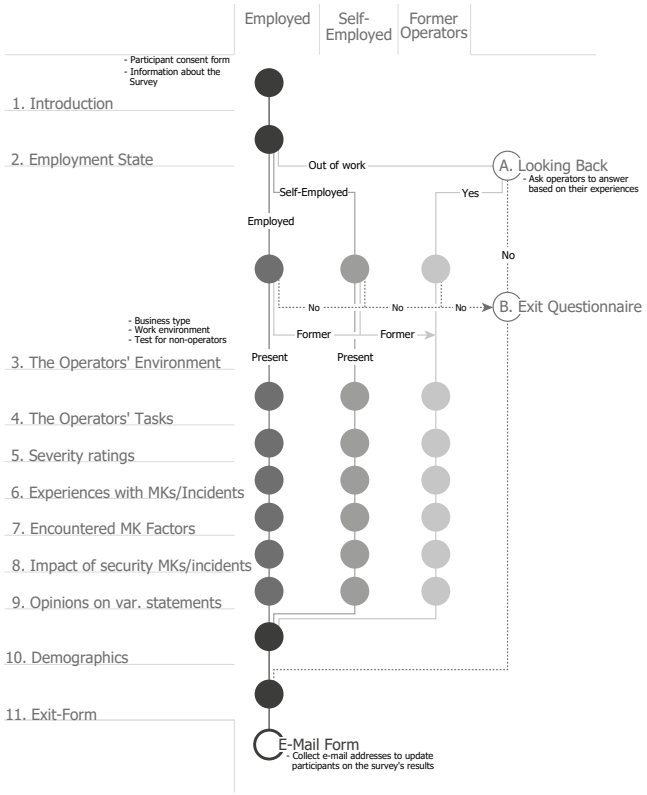


Figure 1: Questionnaire overview

Past Misconfiguration Experience. This section of our questionnaire is dedicated to security misconfigurations and experiences that operators have with them. To collect comparable and correct data, we define and describe what security and security misconfigurations are in the context of the questionnaire. The questions of this section serve to address our observation that security misconfigurations appear to be a common issue in IT operations. Hence, we record whether operators had misconfigured something before that was security-relevant, and whether there had been an incident because of it. Furthermore, based on our observations on the importance of blameless postmortems, we also ask if they had *encountered* a security misconfiguration made by someone else.

To better understand the frequency of different types of misconfigurations, and to compare to the respondents' self-reflections in the first part of this section, we also inquire whether the operators *have encountered* a specific misconfiguration or had *misconfigured a specific system themselves* using examples of misconfigurations from our qualitative study (Table 3). To supplement our qualitative data on how misconfigurations are detected in practice, we also provide an optional free-text field.

Misconfiguration Facilitating Factors. In this part of the survey, we ask operators to indicate how regularly they encountered the *personal*, *environmental* and *system-specific* misconfiguration facilitating factors that we identified in our qualitative study (Section 4). Again, we provide a free-text field to collect additional qualitative data.

Consequences. Investigating consequences of a security misconfiguration incident relates to the reoccurring theme that incidents supposedly change a company's security posture. Hence, we inquire whether the discovery of security misconfigurations resulted in a perceived change in security posture, and whether the operators perceived possible changes as for the better or for the worse. Concerning the influence of a security incident, participants compare the impact of actual security incidents to the mere discovery of misconfigurations. For both questions, they are free to pick *I don't know* if they have no experience or opinion on the matter.

Opinions. The last misconfiguration-related part of our questionnaire addresses the operators' opinions on statements from our qualitative interviews. Questions include, for example, whether the operators felt they were taught how to deal with broken systems over the course of their education, and whether they think that too many options are configurable nowadays ("too many knobs"). Table 4 (Section 6) provides an overview of the statements that we analyze. Furthermore, we inquire which systems they find particularly hard to operate and why (in a free-text field), as they may point at particularly hard-to-use or unpopular systems that researchers should investigate more closely.

Demographics. To allow comparison of our data with other studies, such as the USENIX LISA salary survey among operators [29], we collect demographic data on the participants. This includes their work location, age range, and level of education.

5.2 Dissemination

To increase participation in our study, we established a brand in our dissemination channels to utilize a recognition effect that spans all dissemination channels. We also used this brand in our survey, so that participants recognized our survey throughout different dissemination channels [37]. Establishing a recognizable brand was particularly crucial to recruit system operators, who are more difficult to recruit through traditional mechanisms (e.g., monetarily, due to generally higher compensation) and more time constrained (i.e., they might not participate the first time they encounter the study), because information and reminders about the study were more easily and immediately recognizable. We did this through comics in a distinctive drawing style (e.g., Figure 2). Our drawings also proved useful for illustrating concepts, clarifying definitions, and what we were asking for in the questionnaire. Furthermore, while we did not compensate participants, we provided them the opportunity to be informed about any updates on our research project. To ensure anonymity of survey responses, we collected the email addresses through a separate form, which was fully separated from the survey.

We used a multi-channel approach to disseminate our study directly within the operations community:

(1) A presentation at the 76th RIPE Meeting, which is the regular meeting of the local IP address authority for Europe, the Middle-East, and Russia, where we also used the aforementioned drawing-style to establish the brand, assuming that brand recognition for a funny and appealing presentation [38] might convince operators to participate in our survey [37].

Figure 2: Drawing style example of the questionnaire

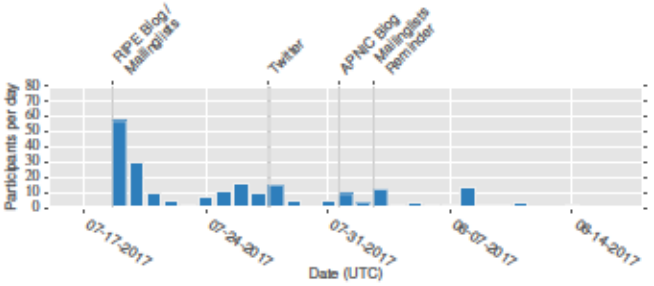


Figure 3: Responses per day

(2) Publishing articles in the blogs of the RIPE NCC [39] and APNIC [40], the latter of which is the address registry for Asia and Oceania.
(3) Sending emails to operations mailing lists with several thousand recipients.
(4) Social media activity in relevant industry communities advertising the survey.

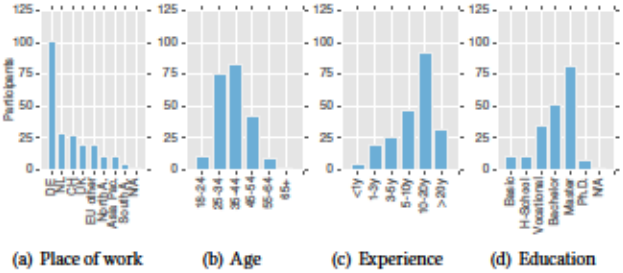
We refrained from utilizing community and "question and answer" sites like Server Fault [41] or Super User [42] because their respective terms of service prohibit advertising or conducting surveys (doing so is often perceived as intrusive by operators). In fact, although we only advertised our survey on mailing lists for which it was allowed, we occasionally received negative feedback that our study was unsolicited. We did not trace participation in the survey to a specific dissemination channel, as we opted to not implement user tracking in our questionnaire due to ethical concerns.

6 QUANTITATIVE RESULTS

Participation. We published our survey on July 19, 2017 and concluded it 30 days later (August 17, 2017). In total, we received 231 responses, 80 percent of which were recorded in the first 15 days. 78 participants subscribed to our mailing list for updates on our findings. Figure 3 shows how our dissemination efforts relate to the number of participants of the questionnaire.

Filtering. We excluded ten responses from our analysis due to incorrect or incomplete data. For four of these ten submissions no data was collected, potentially due to Google Forms malfunctioning. The six other respondents stated they had never worked as operators before, two of which additionally declared that they just liked disrupting surveys. Hence, our analysis is based on the remaining 221 current and former operators.

Demographics. The majority of respondents works in Germany (45.70%), but we also received notable contributions from other parts of Europe, specifically the Netherlands, Switzerland, and the United Kingdom (Figure 4(a)). Likely because our dissemination focused on



(a) Place of work (b) Age (c) Experience (d) Education

Figure 4: Key demographics of the quantitative study

European organizations, other parts of the world are underrepresented. However, considering the increasing internationalization, especially in IT industries, we do not regard this as a significant limitation. That it is not a limitation is also being highlighted by the distribution of age and experience of participants (Figure 4(b) and Figure 4(c)), which is similar to that of other regions, for example, as shown by earlier studies for the U.S.-centric operations community [29]. Concerning the level of education, our results differ: 63.8% of all respondents have at least a Bachelor's degree, which stands in contrast to 41.7% in the last LISA salary survey [29]. Nevertheless, this difference may be due to the eased accessibility and lower personal financial cost of higher education in Europe, possibly because of larger public financial support [43]. These considerations underline that our sample is—within its limitations (Section 8)—representative concerning the underlying strata.

Employment Situation. For the results of our survey, 89.1% of operators are employees, 8.2% are self-employed, and 2.7% are former operators. Notably, nearly half (48.9%) of all participants consider their position to be at least partially a managerial position (e.g., as team leaders). We also find a reasonable variety in terms of industries that the participants work in: Spanning from IT enterprises to ISPs to government organizations and organizations that do not operate in the IT sector, but who rely on IT to support their core business operations.

6.1 Security Misconfiguration Frequency

Our first observation from our qualitative study is that security misconfigurations are an (even more) common issue than reported (security) incidents indicate. Since security misconfigurations carry a certain amount of guilt, operators may not be upfront or honest when being asked about misconfigurations that they personally created (i.e., if there are no "blameless postmortems"). Therefore, we separated the involved responsibility domains (Section 5) and we first asked the operators whether they had misconfigured something themselves, and then whether they had found *somebody else's* misconfiguration.

For the former self-reflective part, we also provided operators with the option to acknowledge that they may have misconfigured something, which they yet have to notice. We also inquired if any of the discovered misconfigurations led to a security incident. Furthermore, to also include cases for which the operators did not fully share our understanding of a security misconfiguration, we subsequently presented them with a list of possible misconfigurations

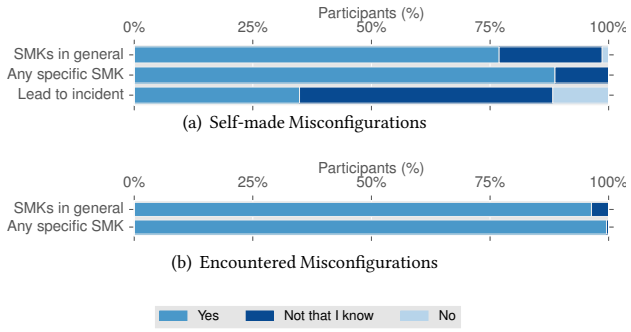


Figure 5: Operators response on whether they conducted misconfigurations (a), or, encountered misconfigurations (b), split by their responses in general and when asking for specific misconfigurations.

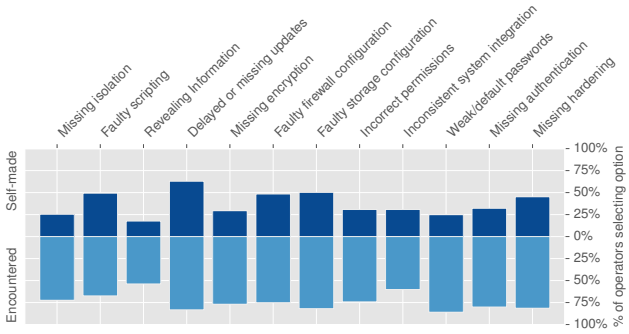


Figure 6: Most common security misconfiguration types operators encountered/did themselves.

based on our qualitative study. Again, we asked whether these misconfigurations had happened to them, and/or, if they encountered them.

From 221 operators, 170 (76.92%) acknowledge that they misconfigured a system and 68 (30.8%) state that at least one misconfiguration led to a security incident (Figure 5). Nine operators (4.1%) state that one of their own security misconfigurations led to a security incident, contradicting their prior statements that they are not aware of security misconfigurations that they committed in the past. This may be explained by different notions of security misconfigurations. If we consider the answers to *specific* incidents, then the number of operators acknowledging their own security misconfigurations rises to 196 (88.7%). Furthermore, when prompting for specific misconfigurations they had encountered, only one operator (0.5%) claims to have never encountered any of the specific misconfigurations we mentioned, or even encountered one in general.

Looking closer at specific *types* of misconfigurations (Table 3), the average operator made more than four different kinds of misconfigurations (4.3) and encountered more than eight (8.4). Out of twelve presented misconfigurations, the most common *self-made* ones are *delayed or missing updates*, *faulty scripting*, and *faulty firewall configuration* (Figure 6). Among the *encountered* misconfigurations, *weak or default passwords*, *delayed or missing updates*, and *faulty assignment of permissions* are the most frequently selected misconfigurations (also Figure 6). The most interesting observation here is that, with a deviation of around 20%, the relative frequency for self-made and encountered misconfigurations match, except for cases that are straight-forward violations of operational best practices (weak or default authentication credentials (password), insufficient security hardening, and misusing systems). We conjecture that the difference may be related to avoidance of negative self-reflection in our participants.

Discussion. Overall, close to all respondents of our survey encountered security sensitive misconfigurations in practice. This corresponds to our qualitative interviews, in which all interview partners encountered misconfigurations and shared a multitude of related experiences. Nevertheless, we see a tendency of operators to be more willing to acknowledge misconfigurations if it does not attribute guilt to them. In line with our qualitative interviews, it *highlights the importance of blameless postmortems*. Concerning misconfiguration types, weak or default passwords, lax permissions, and delayed (security) updates are the most frequent issues, closely followed by insufficient and too permissive firewall rules. Interestingly, these are also the types of misconfigurations that are regularly considered responsible for major data leaks [44].

6.2 Organizational Factors and Management

In our questionnaire, we asked the operators which misconfiguration facilitating factors they identified for misconfigurations that they encountered during their work. The most frequent personal factors are a lack of knowledge (78.73%) and a lack of experience (75.57%), which aligns with our qualitative interviews, where participants frequently mentioned that missing experience and a lack of knowledge are major issues.

In the context of environmental factors, the most frequent reasons are sole responsibility (76.92%) and insufficient quality assurance (73.30%). The general picture here is that during the qualitative interviews, the focus was on *social* issues, while during the questionnaire study organizational aspects appear to stand out. This may be attributable to the different circumstances induced by the qualitative and the quantitative methodology [45], that is, the difference is because social issues are more likely to be voiced during the (seemingly) less formal interviews rather than a survey. This may also play a role in why the usage of defaults is the most common systemic factor, while it was only infrequently mentioned during the interviews: Respondents may not have felt comfortable to discuss it, as it is stigmatized as a form of personal failure.

Turning toward the management, we find that operators consider poor "financial decisions" and "unqualified leadership" less of an issue than the initial qualitative interviews indicated. While our interview partners were quite vivid about their perspective on the quality of their leadership, only little more than a third of operators (39.37%) see unqualified leadership as a cause for security misconfigurations. Similarly, less than a third of respondents (30.77%) point to financial decisions as being a cause for security misconfigurations. Surprisingly, operators seem to agree that their direct supervisors understand what they do (Table 4, line 7).

However, when investigating this opinion more closely, we find that it is impacted by an operator's organizations' type. Operators from organizations without an IT background (avg. 0.534) and the government sector (avg. 0.474) are significantly less convinced that their superiors know what they are doing ($p < 0.05$ in Pearson's χ^2) than those from IT service providers (avg. 0.832) and IT enterprises (avg. 0.810). Similarly, freelancers are less convinced (avg. 0.278) that their direct superiors, that is, their customers, understand what they are doing, compared to employed operators (an average of 0.784 for full-time employees and 0.864 for part-time employees with $p < 0.05$ in Pearson's χ^2). In our sample, the occurrence of freelancers in a company is *not* significantly co-dependent on the sector ($p > 0.15$ in Pearson's χ^2).

Considering results from the *Opinions* section of our survey (Table 4), Statement 10 ("I trust all the tools and equipment we're using.") is of particular interest: Operators seem to generally distrust the tools that they are using and need to rely on, with a global average of -0.651. In fact, it correlates with the operators' experience. "Younger" operators still trust their tools (< 1 year in the field, avg. 0.400), while less junior operators already start to distrust them (1-3 years operating experience, avg. 0.050). After three years of experience in the field, the disagreement rises further (3-5 years experience, avg. -0.462), and the trust only decreases over time, culminating at an average disagreement of -1.032 for operators with more than 20 years experience. This effect is significant at $p < 0.005$ in Pearson's χ^2 and naturally co-correlates with the operators' age.

Discussion. Based on our survey, we can assert that operators see major obstacles for secure operations and preventing security misconfigurations on the organizational side. We also find that the sector of an organization has an impact on the (perceived) IT aptitude of the operators' managers. While this might be expected, we suggest that non-IT organizations take special care to offer additional training for IT middle managers who are promoted into this position from diverse backgrounds. Failing to do so could otherwise result in an environment that facilitates misconfigurations.

Naturally, the focus of strategies to mitigate misconfigurations should be on environmental features: *Reducing sole responsibility, introducing (more) quality assurance and automation*, and, *ensuring that operators do not face unreasonable workloads*. Indeed, several personal factors, while commonly selected, may be co-dependent on organizational factors and might be mitigated indirectly by addressing these organizational factors. For example, a lack of knowledge or experience can be mitigated by reducing sole responsibility and a four-eye policy, especially for sensitive or security-relevant changes and junior operators.

The increasingly dwindling trust of operators in their tools over the course of their careers is also an important matter that needs to be addressed. We conjecture that it is a symptom of getting continuously frustrated with tools not living up to their expectations and promises. Unfortunately, this increasing distrust and reluctance can have negative effects on the deployment of mitigations: If operators do not trust them, then they might not (correctly) deploy them in the first place, or they might try to find ways around them. In fact, this effect corresponds to fundamental conclusions that analyzes of decades of devastating incidents in safety science have made [46].

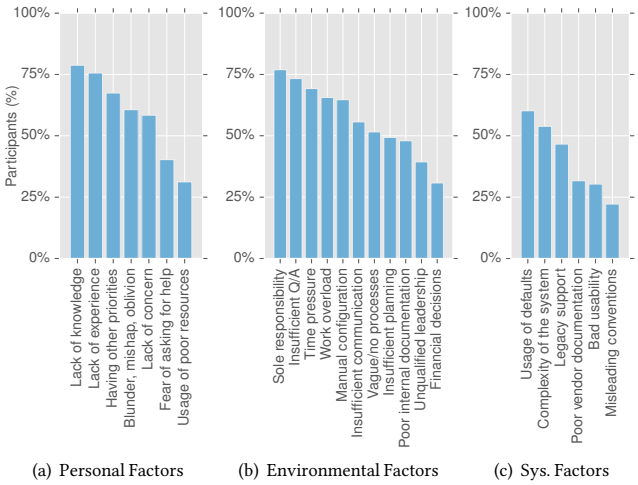


Figure 7: Frequency of misconfiguration facilitating factors based on shares of participants who have encountered misconfigurations with these factors.

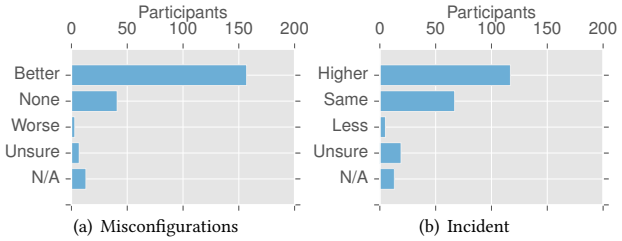


Figure 8: Operators' perceived impact of security misconfigurations and incidents on organizations security posture.

6.3 Incident Response

The third observation that we made based on our qualitative interviews is that operators suggest that a security incident due to a misconfiguration makes management and operations personnel (temporarily) more security sensitive. Asking operators directly, 81.9% either agree or strongly agree that the discovery of a security misconfiguration has made them more security conscious, with 33.0% strongly agreeing to that statement (Table 4 line 4). Similarly, 71% of respondents are convinced that their company's security posture improved after a security misconfiguration was discovered (Figure 8). However, 53% of respondents also report that an actual *incident* had an even higher impact on the organizations' security posture than the discovery of misconfiguration that did not yet cause an incident (Figure 8).

Several operators point out that security-relevant changes are often planned but never implemented, were only active temporarily (lasted for a while, but were then reverted), that management was willing to improve but was unwilling to provide the necessary resources to do so, or that management applied unreasonable security metrics and measures. Some operators also highlight the lack of security awareness and that the lack of distinct responsibilities

No.	Statement	+2	+1	±0	−1	−2	/	Plot (%)	Avg.
1	I feel responsible for keeping my operations secure.	144	67	5	1	1	3		1.615
2	I feel responsible for pointing out security issues to peers.	127	79	8	3	0	4		1.521
3	Blameless postmortems help to detect essential issues in corporate procedures.	95	76	22	6	2	20		1.274
4	The discovery of a security misconfiguration made me more cautious regarding security.	74	107	28	7	0	5		1.148
5	The threat of bad press after a security incident is what companies fear most.	65	85	33	13	2	23		1.000
6	The general priority of security rises after a security incident has happened.	49	100	42	18	2	10		0.834
7	My direct supervisor understands what I'm actually doing.	57	92	30	27	11	4		0.724
8	My direct supervisor knows the amount of work I'm doing.	34	108	30	35	10	4		0.558
9	In my company we keep up with security standards.	33	85	43	38	13	9		0.410
10	I trust all the tools and equipment we're using.	5	30	51	78	51	6		-0.651
11	My company budgets for mistakes (such as misconfigurations and security incidents).	5	21	29	54	58	54		-0.832

Table 4: Overview of responses to opinion-based questions from the survey

contributes further to the problem. One operator adds that companies fear bad press most, a sentiment that operators generally agree with (Table 4, line 5). In general, it points toward an uncoordinated picture of incident response and overall bad security posture in companies, with only half (53.39%) of respondents agreeing that their companies' security postures are sufficient (Table 4, line 9).

Finally, as a measure to correctly handle the aftermath of a misconfiguration incident, 77.4% of our respondents agree that blameless postmortems are important (Table 4, line 3). However, there are significant differences between freelancers (avg. 0.867), and employed system operators (full-time avg. 1.325, part-time avg. 1.400) ($p \leq 0.001$ in Pearson's χ^2). Considering that most companies do not budget for errors (Table 4, line 10), we conjecture that this is due to freelancers serving as easy scapegoats in situations where an organization pretends to perform a blameless ppostmortem

Summary. Overall, our quantitative survey aligns with the operators' suggestions from our qualitative interviews. However, additional qualitative answers by the respondents indicate that even changes that are implemented are not actually permanent, which results in lapses in an organization's security posture. Participants also agree that *blameless postmortems* are fundamental for meaningful, effective, and long-lasting incident response. Unfortunately, for blameless postmortems to have impact, companies must embrace that (human) errors can and will happen, and budget for their eventual occurrence, which currently is not the case. Finally, if postmortems are supposed to be blameless, while still appointing blame, then the impact on moral and their long-term effectiveness might be devastating (e.g., eroding trust in leadership).

7 RELATED WORK

We compare to relevant prior research in four categories: *(i)* studies of misconfigurations and mitigation efforts, *(ii)* usability studies concerned with technical systems creating or preventing errors, *(iii)* studies focusing on personal behavioral causes for security issues, and *(iv)* research in safety sciences.

Misconfigurations and Mitigation. Kuhrer et al. found that large-scale notification campaigns can significantly reduce the number of Internet-connected systems that are misconfigured and could be exploited to act as traffic amplifiers [47], and Czyz et al. reported on a similar effort to reduce the number of NTP amplifiers [48]. However, in 2016, Fiebig et al. showed that such an improvement instances was only temporary for publicly exposed Redis and memcached services [6]. Springall et al. investigated Internet-wide misconfigured publicly accessible FTP servers in 2016, but they did not report whether they notified operators or whether misconfigurations were amended in a temporary or permanent way [49]. Prior work also confirmed that misconfigurations facilitate other equally problematic security issues: mobile applications leaking sensitive and private data [50], applications becoming vulnerable to denial of service attacks [10, 11], websites turning malicious and infecting visitors with malware [12], websites misusing its visitors to mine cryptocurrency [51], and websites being modified to embarrass its operators via defacements [13, 14]. In fact, misconfigurations can even lead to account compromises for some single sign-on protocols [52].

Finding misconfigurations in IPv6 recently lead to more work toward making IPv6 scannable or enumerable [53–55]. Czyz et al. found that the same systems expose insufficiently protected services, i.e. host misconfigured services, more often via IPv6 than via IPv4 [56]. Similar, Borgolte et al. found several thousand critical systems to be misconfigured in regard to their IPv6 security [55]. Interestingly, Zhang et al. identified a correlation between the maliciousness and misconfigurations in networks [57]. Apart from their security impact, misconfigurations have long been an important subject in the networking community: Mahajan et al. conducted a large-scale investigation of BGP misconfigurations in 2002 [58], while Le et al. used data mining to detect router misconfiguration [59]. Streibelt et al. investigated issues around BGP communities [60].

Usability and Technical Mitigations. Xu et al. created a system to detect system design that facilitates misconfiguration and they analyzed the configuration syntax of various popular Internet services [61]. Similarly, already in 2007, Haber et al. distilled design guidelines for system operations tools [62]. In 2015, Xu et al. comprehensively analyzed how systems' complexity leads to security misconfigurations [63], and they survey technical approaches to reduce security misconfigurations [64]. Keller et al. introduced ConfErr to increase the resilience of systems to misconfigurations [65], and Oliveira proposed designing systems that are mistake-aware [66].

Behavioral Studies. Fahl et al. reported on their study among webmasters who run expired TLS certificates [67]. Contrary to our study, participants in the study by Fahl et al. mainly requested technological changes to mitigate these misconfigurations. Krombholz et al. investigated the challenges in configuring TLS correctly in a qualitative study, focusing on the usability aspects of the involved software [9]. Acar et al. conduct a large-scale study on the sources that

Android developers utilize while writing mobile applications, and, thus, might lead to security issues [31]. While orthogonal on first sight, it relates to our observations on operators mentioning *themselves* that misconfigurations are created in part by using online resources that recommend problematic configurations. On the recruiting side of behavioral studies, Acar et al. investigate the challenges in recruiting a meaningful sample of IT professionals via GitHub for studies to understand and improve their security decision-making process [68]. To improve tools used by security operations centers, Sundaramurthy et al. evaluate what inherent conflicts exist in the objectives of security operations centers, how they manifest themselves in inefficiencies, and how they can be resolved effectively [69].

Safety Science. Similar to the current state in computer security and operations, the initial focus in safety science was on the so called "sharp-end," that is individual human error while executing specific actions [70]. However, it became apparent in the 1990s that an approach including organizational aspects and precursors is fundamental to effectively *mitigate* human error: *"Fallibility is here to stay. Organizational and local problems, in contrast, are both diagnosable and manageable."* [70].

A common example illustrating the underlying paradigm shift is the case of *MS Herald of Free Enterprise*, which capsized only moments after departure in Zeebrugge in 1987 because a dockhand forgot to close a shot. The initial report selectively investigated person-centric causes, appointing responsibility to the humans involved. Praetorius et al. re-analyzed this incident 25 years later from a systemic perspective leveraging functional resonance analysis method (FRAM) [71]. They determined that the incident does not have a single cause and that human error is not one of the major causes, but actually the contrary: The human error is a symptom of functional resonance in various functions of the operation of the ship. Similarly, Schröder-Hinrichs et al. investigated large maritime incidents from the *R.M.S. Titanic* to, most recently, the *Costa Concordia*, and found *the same* underlying facilitating factors to be of cause [46].

8 LIMITATIONS

Due to our recruitment strategy (Section 5.2), our study may suffer from (self-)selection bias. Our participants are likely to identify with their work, as they are actively involved in the operators' community. In turn, we may inadvertently exclude less active operators, which may have a different perception. However, as our research also includes qualitative data such as anecdotes, reasoning and opinions, we receive second hand information on the behavior of operators who do not actively participate in the community beyond their "nine-to-five" job (e.g., misconfigurations that operators encountered that they did not do themselves). Although, our sample is comparatively small, our demographic distribution corresponds to that of earlier studies, thus indicating a sufficiently stratified sample [29]. As our analysis is based on self-reported data, it is inherently biased by the participants' perceptions.

9 CONCLUSION

In this paper, we conducted the first systematic study of human aspects of security misconfigurations from the operators' perspective. We find that security misconfigurations do not necessarily lead to incidents: One third of respondents report that the misconfigurations that they witnessed resulted in a security incident, even though all of them *could* have led to a security incident. The observation that almost *all* participants encountered security misconfigurations may be due to a self-selection bias among operators. Specifically, however, given the prevalence of security incidents caused by misconfigurations [2, 3, 44], even considering such a self-selection bias, our data highlights that there is an even larger set of incidents waiting to happen, which could be considerably more disastrous compared to past misconfigurations incidents.

Based on our analysis, we find that human error in system operations is driven by institutional, organizational, and personal factors. Ultimately, to reduce the frequency and impact of security misconfigurations, we recommend the subsequent *immediate action items* that our study highlighted as necessary and useful, which are (unfortunately) rarely implemented by organizations although they are often technically sound and well-known:

Documentation.
The state of any system and all of its components must be properly documented, so that anyone can *fully* understand it. Documentation must be updated immediately upon any changes, and it must be regularly verified for correctness.

Clear Responsibilities.
Organizations must ensure that there is a single responsible department for the security of each device, which has sufficient *authority* over the device to ensure its appropriate security posture. No person shall bear sole responsibility, but responsibility must be shared among multiple people. Organizations, especially outside of the IT sector, must also ensure that their responsible middle management is qualified.

Blameless Post-Mortems.
After an incident occurred, its root cause must be understood, and actions must be taken to prevent a similar incident in the future. While companies appear to embrace a general post-mortem culture, our results indicate that this does not necessarily mean that postmortems are blameless. Hence, the incident postmortem must be constructive and, most important, not appoint blame. To encourage blameless postmortems, we urge organizations to budget for failure and errors.

Processes and Procedures.
All manual changes to the system must be planned. Frequent modifications or configuration changes should be eliminated, or automated and described in a process.

Automation.
Infrastructure and procedures shall be automated, to allow operators to adopt (complex) procedures more easily. For example, canary deployments and rollback plans can highlight and tackle misconfigurations quickly. They have prohibitively high cost if done manually, but they can often be automated, thus highlighting the benefits of automation [72]. Nonetheless, these tools must be engineered to be reliable and should not be a burden on operators. Software and protocols used should be "secure by default" [33]. Considering the increasing distrust in tools with operators' experience, this area requires more work to regain the operators' trust into available tools, as well as to increase the tools' trustworthiness.

Fire Drills.
Regular exercises ("fire drills") shall also be performed to understand the security implications of the current system, how

it can be improved, and to train operators and management in proper incident handling procedures. Ultimately, fire drills can help managers from different backgrounds to better understand the implications of IT operations.

ACKNOWLEDGEMENTS

We thank the anonymous reviewers for their helpful suggestions to improve the paper. We also thank Sascha Fahl for his valuable feedback. We are grateful to the RIPE Academic Initiative (RACI) for supporting this research project with a full scholarship to attend RIPE 76, as well as RIPE NCC and APNIC for helping us disseminate our survey via their blogs. We also extend our gratitude to the German Network Operators Group (DENOG), who supported our research and provided valuable feedback from the early stages.

This material is partially funded by SBA Research. The competence center SBA Research (SBA-K1) is funded within the framework of COMET – Competence Centers for Excellent Technologies by the Austrian Ministry for Transport, Innovation and Technology (BMVIT), the Austrian Federal Ministry for Digital and Economic Affairs (BMDW), and the federal state of Vienna, managed by the Austrian Research Promotion Agency (FFG).

REFERENCES

[1] A. Bühl. *Stellungnahme zum Antisemitismus des Peter Beuth (1781 – 1853)*. June 1, 2017. URL: http://www.beuth-hochschule.de/fileadmin/oe/praesidium/portraet/beuth-diskurs/Beuth_Stellungnahme_Buehl.pdf.

[2] T. Moore. "On the Harms Arising from the Equifax Data Breach of 2017". In: *International Journal of Critical Infrastructure Protection* 19.C (Dec. 2017). DOI: 10.1016/j.ijcip.2017.10.004.

[3] D. Hedley and M. Jacobs. "The shape of things to come: the Equifax breach, the GDPR and open-source security". In: *Computer Fraud & Security* 2017.11 (Nov. 2017). DOI: 10.1016/S1361-3723(17)30080-5.

[4] R. Brandom. *Former Equifax CEO blames breach on a single person who failed to deploy patch*. Oct. 3, 2017. URL: https://www.theverge.com/2017/10/3/16410806/equifax-ceo-blame-breach-patch-congress-testimony (visited on 11/29/2017).

[5] K. Borgolte, T. Fiebig, S. Hao, C. Kruegel, and G. Vigna. "Cloud Strife: Mitigating the Security Risks of Domain-Validated Certificates". In: *Proceedings of the 25th Network and Distributed System Security Symposium (NDSS)*. Feb. 2018. DOI: 10.14722/ndss.2018.23327.

[6] T. Fiebig, A. Feldmann, and M. Petschick. "A One-Year Perspective on Exposed In-memory Key-Value Stores". In: *Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense (SafeConfig)*. Oct. 24, 2016. DOI: 10.1145/2994475.2994480.

[7] B. Rossi. *Major security alert as 40,000 MongoDB databases left unsecured on the Internet*. Feb. 10, 2015. URL: http://www.information-age.com/major-security-alert-40000-mongodb-databases-left-unsecured-internet-123459001/ (visited on 10/25/2017).

[8] S. Ragan. *MongoDB configuration error exposed 93 million Mexican voter records*. Apr. 22, 2016. URL: https://www.csoonline.com/article/3060204/security/mongodb-configuration-error-exposed-93-million-mexican-voter-records.html (visited on 10/25/2017).

[9] K. Krombholz, W. Mayer, M. Schmiedecker, and E. Weippl. ""I Have No Idea What I'm Doing"-On the Usability of Deploying HTTPS". In: *Proceedings of the 26th USENIX Security Symposium (USENIX Security)*. Aug. 2017. URL: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/krombholz.

[10] T. Spring. *Misconfigured Memcached Servers Abused to Amplify DDoS Attacks*. Threatpost. Feb. 28, 2018. URL: https://threatpost.com/misconfigured-memcached-servers-abused-to-amplify-ddos-attacks/130150/ (visited on 08/05/2018).

[11] W. Meng, C. Qian, S. Hao, K. Borgolte, G. Vigna, C. Kruegel, and W. Lee. "Rampart: Protecting Web Applications from CPU-Exhaustion Denial-of-Service Attacks". In: *Proceedings of the 27th USENIX Security Symposium (USENIX Security)*. Aug. 2018. URL: https://www.usenix.org/conference/usenixsecurity18/presentation/meng.

[12] K. Borgolte, C. Kruegel, and G. Vigna. "Delta: Automatic Identification of Unknown Web-based Infection Campaigns". In: *Proceedings of the 20th ACM SIGSAC Conference on Computer and Communications Security (CCS)*. Nov. 2013. DOI: 10.1145/2508859.2516725.

[13] K. Borgolte, C. Kruegel, and G. Vigna. "Meerkat: Detecting Website Defacements through Image-based Object Recognition". In: *Proceedings of the 24th USENIX Security Symposium (USENIX Security)*. Aug. 2015. URL: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/borgolte.

[14] F. Maggi, M. Balduzzi, R. Flores, L. Gu, and V. Ciancaglini. "Investigating Web Defacement Campaigns at Large". In: *Proceedings of the 13th ACM ASIA Conference on Computer and Communications Security (ASIACCS)*. June 2018. DOI: 10.1145/3196494.3196542.

[15] M. Bailey, D. Dittrich, E. Kenneally, and D. Maughan. "The Menlo Report". In: *IEEE Security & Privacy* 10.2 (Mar. 2012). DOI: 10.1109/MSP.2012.52.

[16] D. Dittrich and E. Kenneally. *The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research*. Tech. rep. U.S. Department of Homeland Security, Aug. 2012. URL: https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803_1.pdf.

[17] C. Herley and P. C. van Oorschot. "SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit". In: *Proceedings of the 38th IEEE Symposium on Security & Privacy (S&P)*. May 2017. DOI: 10.1109/SP.2017.38.

[18] Provalis Research. *QDA Miner Lite – Free Qualitative Data Analysis Software*. URL: https://provalisresearch.com/products/qualitative-data-analysis-software/freeware/ (visited on 09/13/2017).

[19] S. B. Merriam and E. J. Tisdell. *Qualitative Research: A Guide to Design and Implementation*. 4th ed. Jossey-Bass, Aug. 24, 2015. ISBN: 978-1119003618.

[20] K. Charmaz. *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*. SAGE Publications, Jan. 27, 2006. ISBN: 978-0761973522.

[21] J. Lazar, J. H. Feng, and H. Hochheiser. *Research Methods in Human-Computer Interaction*. 2nd ed. Morgan Kaufmann, May 3, 2017. ISBN: 978-0128053904.

[22] B. G. Glaser and A. L. Strauss. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Transaction Publishers, 1967. ISBN: 978-0202302607.

[23] A. Strauss and J. Corbin. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. SAGE Publications, Sept. 1, 1990. ISBN: 978-0803932517.

[24] B. G. Glaser. *Basics of Grounded Theory Analysis: Emergence vs Forcing*. Sociology Press, Dec. 1, 1992. ISBN: 978-1884156007.

[25] A. Naiakshina, A. Danilova, C. Tiefenau, M. Herzog, S. Dechand, and M. Smith. "Why Do Developers Get Password Storage Wrong? A Qualitative Usability Study". In: *Proceedings of the 24th ACM SIGSAC Conference on Computer and Communications Security (CCS)*. Oct. 2017. DOI: 10.1145/3133956.3134082.

[26] V. Braun and V. Clarke. "Using thematic analysis in psychology". In: *Qualitative Research in Psychology* 3.2 (2006). DOI: 10.1191/1478088706qp063oa.

[27] Y. Acar, S. Fahl, and M. L. Mazurek. "You are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy Research Beyond End Users". In: *Proceedings of the 1st IEEE Cybersecurity Development (SecDev)*. Nov. 2016. DOI: 10.1109/SecDev.2016.013.

[28] G. Halprin. *The Work Flow of System Administration*. Tech. rep. The SysAdmin Group, June 25, 1998. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.126.3466&rep=rep1&type=pdf.

[29] USENIX LISA. *USENIX Special Interest Group for Sysadmins: The 2011 Salary Survey*. 2011. URL: https://www.usenix.org/sysadmin-salary-surveys (visited on 11/29/2017).

[30] R. Dhamija, J. D. Tygar, and M. Hearst. "Why Phishing Works". In: *Proceedings of the 2006 ACM SIGCHI Conference on Human Factors in Computing Systems*. Apr. 2006. DOI: 10.1145/1124772.1124861.

[31] Y. Acar, M. Backes, S. Fahl, D. Kim, M. L. Mazurek, and C. Stransky. "You Get Where You're Looking For: The Impact Of Information Sources on Code Security". In: *Proceedings of the 37th IEEE Symposium on Security & Privacy (S&P)*. May 2016. DOI: 10.1109/SP.2016.25.

[32] J. J. Francis, M. Johnston, C. Robertson, L. Glidewell, V. Entwistle, M. P. Eccles, and J. M. Grimshaw. "What is an adequate sample size? Operationalising data saturation for theory-based interview studies". In: *Psychology & Health* 25.10 (2010). DOI: 10.1080/08870440903194015.

[33] T. Fiebig, F. Lichtblau, F. Streibelt, T. Krüger, P. Lexis, R. Bush, and A. Feldmann. "Learning from the Past: Designing Secure Network Protocols". In: *Cybersecurity Best Practices*. 2018.

[34] Ponemon Institute. *2017 Cost of Data Breach Study: Global Overview*. Tech. rep. IBM, July 2017. URL: https://www.ibm.com/security/data-breach.

[35] Google LLC. *Google Forms - create and analyze surveys, for free*. URL: https://www.google.com/forms/about/ (visited on 10/03/2017).

[36] R. Likert. "A Technique for the Measurement of Attitudes". In: *Archives of Psychology* 22.140 (1932). LCCN: 33012634.

[37] T.-M. Karjalainen and D. Snelders. "Designing Visual Recognition for the Brand". In: *Journal of Product Innovation Management* 27.1 (Jan. 2010). DOI: 10.1111/j.1540-5885.2009.00696.x.

[38] C. Dietrich. *Caught between Security and Time Pressure*. Presentation at RIPE 74. May 9, 2017. URL: https://ripe74.ripe.net/archives/video/54/.

[39] C. Dietrich. *On the Operators' Perspective on Security Misconfigurations – The Survey*. RIPE Labs Blog. July 17, 2017. URL: https://labs.ripe.net/Members/constanze_dietrich/on-the-operators-perspective-on-security-misconfigurations-the-survey.

[40] C. Dietrich. *Survey: Operators' perspective on security misconfigurations.* APNIC Blog. Aug. 1, 2017. URL: https://blog.apnic.net/2017/08/01/survey-operators-perspective-security-misconfigurations/.
[41] Stack Exchange. *ServerFault.* URL: https://serverfault.com/ (visited on 10/23/2017).
[42] Stack Exchange. *Super User.* URL: https://superuser.com/ (visited on 10/23/2017).
[43] G. Brunello and R. Winter-Ebmer. "Why Do Students Expect to Stay Longer in College? Evidence from Europe". In: *Economics Letters* 80.2 (Aug. 2003). DOI: 10.1016/S0165-1765(03)00086-7.
[44] T. Fiebig. "An empirical evaluation of misconfiguration in Internet services". PhD thesis. Technical University of Berlin, Berlin, Germany, Sept. 8, 2017. DOI: 10.14279/depositonce-6140.
[45] J. A. Holstein and J. F. Gubrium. *The Active Interview.* SAGE Publications, Apr. 20, 1995. ISBN: 978-0803958951.
[46] J.-U. Schröder-Hinrichs, E. Hollnagel, and M. Baldauf. "From Titanic to Costa Concordia—a century of lessons not learned". In: *WMU Journal of Maritime Affairs* 11.2 (Oct. 1, 2012). DOI: 10.1007/s13437-012-0032-3.
[47] M. Kührer, T. Hupperich, C. Rossow, and T. Holz. "Exit from Hell? Reducing the Impact of Amplification DDoS Attacks". In: *Proceedings of the 23rd USENIX Security Symposium (USENIX Security).* Aug. 2014. URL: https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/kuhrer.
[48] J. Czyz, M. Kallitsis, M. Gharaibeh, C. Papadopoulos, M. Bailey, and M. Karir. "Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks". In: *Proceedings of the 2014 Internet Measurement Conference (IMC).* Nov. 2014. DOI: 10.1145/2663716.2663717.
[49] D. Springall, Z. Durumeric, and J. A. Halderman. "FTP: The Forgotten Cloud". In: *Proceedings of the 46th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN).* June 2016. DOI: 10.1109/DSN.2016.52.
[50] J. Ren, M. Lindorfer, D. Dubois, A. Rao, D. Choffnes, and N. Vallina-Rodriguez. "Bug Fixes, Improvements, ... and Privacy Leaks – A Longitudinal Study of PII Leaks Across Android App Versions". In: *Proceedings of the 25th Network and Distributed System Security Symposium (NDSS).* Feb. 2018. DOI: 10.14722/ndss.2018.23143.
[51] R. K. Konoth, E. Vineti, V. Moonsamy, M. Lindorfer, C. Kruegel, H. Bos, and G. Vigna. "MineSweeper: An In-depth Look into Drive-by Cryptocurrency Mining and Its Defense". In: *Proceedings of the 25th ACM SIGSAC Conference on Computer and Communications Security (CCS).* Oct. 2018. DOI: 10.1145/3243734.3243858.
[52] Y. Cao, Y. Shoshitaishvili, K. Borgolte, C. Kruegel, G. Vigna, and Y. Chen. "Protecting Web Single Sign-on against Relying Party Impersonation Attacks through a Bi-directional Secure Channel with Authentication". In: *Proceedings of the 17th International Symposium on Recent Advances in Intrusion Detection (RAID).* Sept. 2014. DOI: 10.1007/978-3-319-11379-1_14.
[53] O. Gasser, Q. Scheitle, S. Gebhard, and G. Carle. "Scanning the IPv6 Internet: Towards a Comprehensive Hitlist". In: *Proceedings of the 2016 International Workshop on Traffic Monitoring and Analysis (TMA).* arXiv: 1607.05179v1. Apr. 2016.
[54] T. Fiebig, K. Borgolte, S. Hao, C. Kruegel, and G. Vigna. "Something From Nothing (There): Collecting Global IPv6 Datasets From DNS". In: *Proceedings of the 12th Passive and Active Measurement (PAM).* Mar. 2017. DOI: 10.1007/978-3-319-54328-4_3.
[55] K. Borgolte, S. Hao, T. Fiebig, and G. Vigna. "Enumerating Active IPv6 Hosts for Large-scale Security Scans via DNSSEC-signed Reverse Zones". In: *Proceedings of the 39th IEEE Symposium on Security & Privacy (S&P).* May 2018. DOI: 10.1109/SP.2018.00027.
[56] J. Czyz, M. Luckie, M. Allman, and M. Bailey. "Don't Forget to Lock the Back Door! A Characterization of IPv6 Network Security Policy". In: *Proceedings of the 23rd Network and Distributed System Security Symposium (NDSS).* Feb. 2016. DOI: 10.14722/ndss.2016.23047.
[57] J. Zhang, Z. Durumeric, M. Bailey, M. Liu, and M. Karir. "On the Mismanagement and Maliciousness of Networks". In: *Proceedings of the 21st Network and Distributed System Security Symposium (NDSS).* Feb. 2014. DOI: 10.14722/ndss.2014.23057.
[58] R. Mahajan, D. Wetherall, and T. Anderson. "Understanding BGP misconfiguration". In: *Proceedings of the 2002 ACM SIGCOMM Conference (SIGCOMM).* Aug. 2002. DOI: 10.1145/633025.633027.
[59] F. Le, S. Lee, T. Wong, H. S. Kim, and D. Newcomb. "Minerals: Using Data Mining to Detect Router Misconfigurations". In: *Proceedings of the 2016 Workshop on Mining Network Data (MineNet).* Sept. 15, 2006. DOI: 10.1145/1162678.1162681.
[60] F. Streibelt, F. Lichtblau, R. Beverly, A. Feldmann, C. Pelsser, G. Smaragdakis, and R. Bush. "BGP Communities: Even more Worms in the Routing Can". In: *Proceedings of the 2018 Internet Measurement Conference (IMC).* Nov. 2018.
[61] T. Xu, J. Zhang, P. Huang, J. Zheng, T. Sheng, D. Yuan, Y. Zhou, and S. Pasupathy. "Do Not Blame Users for Misconfigurations". In: *Proceedings of the 24th ACM Symposium on Operating Systems Principles (SOSP).* Nov. 2013. DOI: 10.1145/2517349.2522727.
[62] E. M. Haber and J. Bailey. "Design Guidelines for System Administration Tools Developed Through Ethnographic Field Studies". In: *Proceedings of the 2007 ACM Symposium on Computer Human Interaction for the Management of Information Technology (CHMIT).* Mar. 2007. DOI: 10.1145/1234772.1234774.
[63] T. Xu, L. Jin, X. Fan, Y. Zhou, S. Pasupathy, and R. Talwadker. "Hey, You Have Given Me Too Many Knobs!: Understanding and Dealing with Over-designed Configuration in System Software". In: *Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering (ESEC/FSE).* Aug. 2015. DOI: 10.1145/2786805.2786852.
[64] T. Xu and Y. Zhou. "Systems Approaches to Tackling Configuration Errors: A Survey". In: *ACM Computing Surveys* 47.4 (July 2015). DOI: 10.1145/2791577.
[65] L. Keller, P. Upadhyaya, and G. Candea. "ConfErr: A Tool for Assessing Resilience to Human Configuration Errors". In: *Proceedings of the 38th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN).* June 2008. DOI: 10.1109/DSN.2008.4630084.
[66] F. A. D. de Oliveira. "Towards Mistake-Aware Systems". PhD thesis. Rutgers University, New Brunswick, New Jersey, Oct. 2010. DOI: 10.7282/T3N58M3J.
[67] S. Fahl, Y. Acar, H. Perl, and M. Smith. "Why Eve and Mallory (Also) Love Webmasters: A Study on the Root Causes of SSL Misconfigurations". In: *Proceedings of the 9th ACM ASIA Conference on Computer and Communications Security (ASIACCS).* July 2014. DOI: 10.1145/2590296.2590341.
[68] Y. Acar, C. Stransky, D. Wermke, M. L. Mazurek, and S. Fahl. "Security Developer Studies with GitHub Users: Exploring a Convenience Sample". In: *Proceedings of the 13th Symposium On Usable Privacy and Security (SOUPS).* June 2017. URL: https://www.usenix.org/conference/soups2017/technical-sessions/presentation/acar.
[69] S. C. Sundaramurthy, J. McHugh, X. Ou, M. Wesch, A. G. Bardas, and S. R. Rajagopalan. "Turning Contradictions into Innovations or: How We Learned to Stop Whining and Improve Security Operations". In: *Proceedings of the 12th Symposium On Usable Privacy and Security (SOUPS).* June 2016. URL: https://www.usenix.org/conference/soups2016/technical-sessions/presentation/sundaramurthy.
[70] J. Reason. "Safety in the operating theatre – Part 2: Human error and organisational failure". In: *Quality and Safety in Health Care* 14.1 (Feb. 2005). DOI: 10.1016/S0953-7112(05)80010-9.
[71] G. Praetorius, M. Lundh, and M. Lützhöft. "Learning From The Past For Pro-activity – A Re-analysis Of The Accident Of The MV Herald Of Free Enterprise". In: *Proceedings of the 4th Resilience Engineering Symposium.* June 2011. DOI: 10.4000/books.pressesmines.1089.
[72] T. A. Limoncelli, C. J. Hogan, and S. R. Chalup. *The Practice of System and Network Administration: Volume 1: DevOps and other Best Practices for Enterprise IT.* 3rd ed. Addison-Wesley Professional, Nov. 14, 2016. ISBN: 978-0321919168.

A QUESTIONNAIRE

The questionnaire uses the following structure: Questions in bold are required. Circles denote single selection answers. Boxes denote optional multiple selection answers. Tables with circles denote single response per row. Tables with boxes denote optional multiple responses per row. Questions without selections allow free text answers.
Please note: The wording of this example questionnaire is for employees. In our study, participants were shown specific wording based on their selection during "For Starters."

Welcome Page

Misconfigurations happen

We are all human beings and we make mistakes. (At least I'm fairly sure I'm not the only one.) Therefore, we assume that faulty security configurations that may lead or even have lead to leaked, lost or distorted data must be a lot more common than we perceive them to be. We want to explore what experiences YOU, the operators, have had with misconfigurations - regardless of whether they happened to yourselves, you discovered them or you were the ones fixing them.
We also believe that knowing how they occur may allow for measures to reduce the risk of misconfigurations - measures not only addressing the operators, but all departments through all levels of management that affect the design and maintenance of a system in some way. Therefore, the

following questions aren't designed to only gather abstract data but to also incorporate your personal views and opinions - if you want. :)
This survey is the main task of my master thesis in media informatics at the Beuth University of Applied Sciences in collaboration with the Technical University Berlin.[2]
Your answers remain entirely anonymous. We're not aiming for sensitive information. Nevertheless, be assured that we hold ourselves responsible for preserving your anonymity.

We need you!

We already learned that operators are usually quite busy operating things; but if you can spare 10 to 20 minutes to fill out this questionnaire, please do! Each and every contribution is important and helps us and eventually fellow operators a lot!

PS

If you'd like to get brief updates and a summary of our findings, you may leave your email adress at the end of the survey in a separate form. Also, if you happen to answer these questions on your phone, they render best after switching to landscape mode.

For Starters

To make the questions serve your current situation.

(1) **Are you employed, self-employed or out of work?** If you're a student, please choose what you do besides studying.
- ○ I'm employed part-time.
- ○ I'm employed full-time.
- ○ I'm my own boss.
- ○ I do not work at the moment.

Your Job

To get an idea of what you're dealing with day by day.

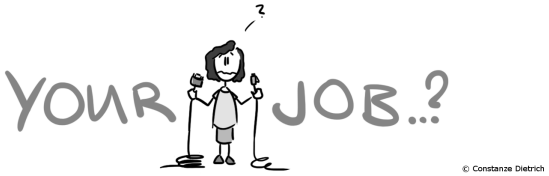
(1) What is your current job title?
(2) Does your job title match what you're actually doing?
- ○ YES.
- ○ More or less.
- ○ NO.

(3) **What kind of business do you work for?** Please refer to the core business of the company you work for.
- ○ IT Service Provider (such as internet, network, storage, application as a service).
- ○ IT Enterprise (e.g. software company).
- ○ Non-IT Enterprise (core businesses other than IT).
- ○ Government/ Public Services.

(4) **What is the approximate total number of employees your company has?**
- ○ 1 - 3
- ○ 4 - 9
- ○ 10 - 49
- ○ 50 - 999
- ○ 1,000 - 4,999
- ○ 5,000 or more
- ○ I don't know.

(5) **Job titles aside – Do you operate IT systems?** Do you consider yourself an operator or have you worked as an operator before?
- ○ YES, I work as an operator.
- ○ YES, but it's not my main task.
- ○ NO, but I worked as an operator before.
- ○ NO. Never. But I like trolling surveys.

Your Job #2



(1) **What kind of IT systems do you operate how often?**

	Never	Rarely	Occasionally	Often	Very often
Computer Operating Systems	○	○	○	○	○
Storage Systems	○	○	○	○	○
Database Systems	○	○	○	○	○
Web Server / Mail Systems	○	○	○	○	○
Networks / Infrastructure	○	○	○	○	○

(2) **How would you describe your level of expertise in operating these systems?**

	No expertise	Very little expertise	Some expertise	Quite a bit of expertise	Very much expertise
Computer Operating Systems	○	○	○	○	○
Storage Systems	○	○	○	○	○
Database Systems	○	○	○	○	○
Web Server / Mail Systems	○	○	○	○	○
Networks / Infrastructure	○	○	○	○	○

(3) **How much of your work is "operating"?**
- ○ 10%
- ○ 20%
- ○ 30%
- ○ 40%
- ○ 50%
- ○ 60%
- ○ 70%
- ○ 80%
- ○ 90%
- ○ 100%
- ○ More than 100%

(4) What kind of tasks do you do besides operating?
(5) **How long have you worked as an operator overall?**
- ○ Less than 1 year.

[2] Affiliation changed to TU Delft before the research project was completed.

- ○ 1 up to 3 years.
- ○ More than 3 up to 5 years.
- ○ More than 5 up to 10 years.
- ○ More than 10 up to 20 years.
- ○ More than 20 years.

(6) **Is your job a management position?** Do you get to make decisions on budget, equipment, staffing...?
- ○ YES.
- ○ More or less.
- ○ NO.

Issues

To get you in the right mood.

(1) How would you rate the severity of each of the following scenarios? Imagine any kind of company with 1,000 employees and 100,000 users. See Table 5.

Your Experiences

We focus on deficient configurations that affect the security of a system. Hence, when answering these questions concerning misconfigurations, please check whether CONFIDENTIALITY, INTEGRITY or AVAILABILITY may have gotten compromised or actually were compromised (and therewith led to a security incident).

(1) **Have you misconfigured something that was relevant for the security of a system?** Regardless of whether there were consequences – Have you ever misconfigured something that affected security?
- ○ YES.
- ○ Not that I'm aware of.
- ○ NO. Never.

(2) **Have you misconfigured something that eventually led to a security incident?** Security incidents might be: Attempts from unauthorized sources to access systems or data/ unplanned disruption to a service or denial of a service/ unauthorized processing or storage of data/ unauthorized changes to system hardware, firmware, or software/ ...
- ○ YES.
- ○ Not that I'm aware of.
- ○ NO.

(3) **Have you ever encountered a security misconfiguration made by someone else?**
- ○ YES.
- ○ Not that I'm aware of.
- ○ NO.

(4) Which of these common security misconfigurations did you make yourself and/or have you encountered done by someone else? Please make sure that the misconfigurations that come to your mind were actually security-related.

	Happened to me.	I have encountered.
Bad or publicly known passwords	□	□
Faulty or missing authentication	□	□
Faulty assignment of permissions	□	□
Delayed or missing updates	□	□
Faulty firewall configuration	□	□
Faulty scripting	□	□
Faulty storage configuration (e.g no safe backups)	□	□
Missing encryption	□	□
Faulty or no hardening (e.g. unneeded ports left open)	□	□
Deployment of revealing information (e.g. extended logfiles)	□	□
Inconsistent system integration	□	□
Misused or improperly shared system (e.g. test/productive, internal/external)	□	□

(5) What other security misconfigurations did you make or encounter? Did we miss something?

(6) How did you come across those security misconfigurations you encountered? Did you stumble upon them while working? Were they discovered while troubleshooting a security incident? Did you spot a ticket/issue?

(7) How many of the security misconfigurations that led to a security incident were known beforehand?
Out of all the security incidents caused by misconfigurations, in how many cases was the misconfiguration already recognized before the incident happened?
- ○ None of them.
- ○ Few of them.
- ○ Half of them.
- ○ Most of them.
- ○ All of them.
- ○ I'm not sure. / Does not apply.

Reasons

(1) Which of the following individual reasons actually have been reasons for security misconfigurations you either did yourself or you have encountered?
- □ Lack of experience
- □ Lack of knowledge
- □ Blunder, mishap, oblivion
- □ Usage of poor (online) resources
- □ Fear of asking for help
- □ Having other priorities
- □ Lack of concern

(2) Were there environmental reasons?
- □ Insufficient or no quality assurance (testing, scanning)

- ☐ Sole responsibility/no review (e.g. peer review)
- ☐ Manual configuration (as opposed to automation)
- ☐ Insufficient (corporate) documentation
- ☐ Insufficient communication
- ☐ Vague or undefined operating procedures
- ☐ Insufficient or no preliminary planning
- ☐ Financial decisions
- ☐ Unqualified leadership
- ☐ Time pressure
- ☐ Work overload

(3) Were there system-specific reasons?
- ☐ Complexity of the system
- ☐ Poor manufacturer's/vendor's documentation
- ☐ Bad usability
- ☐ Usage of defaults
- ☐ Uncommon conventions
- ☐ Legacy support issues

(4) What other reasons did we miss? Since it's impossible to list them all: Which reasons would you take into account here?

Reactions

(1) Given the reasons for security misconfigurations – did something get changed after their discovery? How did your company respond to the security misconfiguration? If there were several cases of security misconfigurations that had quite different outcomes, please refer to your overall impression.
- ○ YES. There were adjustments and it got BETTER overall.
- ○ NO. Basically nothing changed.
- ○ YES. There were adjustments and it got WORSE overall.
- ○ I don't know.
- ○ Other: (free text answer)

(2) How would you describe the impact of actual security incidents on the management? Compared to security misconfigurations without serious consequences – do actual security incidents like data breaches or service outages affect the impact on security-related business decisions?
- ○ LESS. After a security incident the management is less likely willing to improve security.
- ○ SAME. The impact is the same as for security misconfigurations without serious consequences.
- ○ HIGHER. After a security incident the management is most likely willing to improve security.

Your Opinion

- ○ I don't know.
- ○ Other: (free text answer)

(3) If you would like to go into detail… Is there something you would like to remark on that topic?

(1) To what extent would you agree with the following statements? See Table 6.

(2) What software or hardware do you find especially hard to operate? And why? Is there something that seriously annoys you every time you have to touch it? For what reason?

Demographics

(1) **How old are you?**
- ○ Under 18 years.
- ○ 18-24 years.
- ○ 25-34 years.
- ○ 35-44 years.
- ○ 45-54 years.
- ○ 55-64 years.
- ○ 65 years or older.

(2) What is the highest degree or level of education you have completed?
- ○ Some high school, no diploma.
- ○ High school diploma or the equivalent (for example: GED).
- ○ Some college courses, no degree.
- ○ Career/technical/vocational education.
- ○ Bachelor's/undergraduate degree.
- ○ Master's/graduate/professional degree.
- ○ Doctorate/post-graduate degree.
- ○ Other: (free text answer)

(3) **In which country do you work?**

	Very low	Low	Medium	High	Critical
Email addresses of 1000 users got leaked.	○	○	○	○	○
100 users report their accounts have been disabled.	○	○	○	○	○
100 users lose one hour of work done.	○	○	○	○	○
10 non-operator work stations have administrator rights.	○	○	○	○	○
100 users report the data they're seeing isn't theirs.	○	○	○	○	○
Email addresses of all 100,000 users got leaked.	○	○	○	○	○
For one hour 100 employees are unable to login to their work stations.	○	○	○	○	○
10 employees report the database does not show yesterday's changes.	○	○	○	○	○
Work station login data of 100 employees is stored in a physical folder in a one-man office (on paper).	○	○	○	○	○
Credit card information of 1000 users got leaked.	○	○	○	○	○
The backup doesn't match the actual data.	○	○	○	○	○
The corporate mail server fails to filter certain spam.	○	○	○	○	○

Table 5: How would you rate the severity of each of the following scenarios? Imagine any kind of company with 1,000 employees and 100,000 users.

	I strongly agree.	I agree.	I neither agree nor disagree.	I disagree.	I strongly disagree.	I don't now.
My direct supervisor understands what I'm actually doing.	○	○	○	○	○	○
My direct supervisor knows the amount of work I'm doing.	○	○	○	○	○	○
The general priority of security rises after a security incident has happened.	○	○	○	○	○	○
The obligation to report certain security incidents is often not taken serious.	○	○	○	○	○	○
They taught me how to take care of misconfigured systems in school.	○	○	○	○	○	○
I trust all the tools and equipment we're using.	○	○	○	○	○	○
The discovery of a security misconfiguration made me more cautious regarding security.	○	○	○	○	○	○
In my company we keep up with security standards.	○	○	○	○	○	○
Too many things are configurable.	○	○	○	○	○	○
Blameless postmortems help to detect essential issues in corporate procedures.	○	○	○	○	○	○
In my company we have a budget for mistakes (such as misconfiguratins and security incidents).	○	○	○	○	○	○
I feel responsible for keeping my operations secure.	○	○	○	○	○	○
I feel responsible for pointing out security issues to peers.	○	○	○	○	○	○
Software or hardware being certified means it is secure.	○	○	○	○	○	○
Former operators in management allow for more reasonable security-related business decisions.	○	○	○	○	○	○
Agility is more important than security.	○	○	○	○	○	○
The threat of bad press after a security incident is what companies fear most.	○	○	○	○	○	○

Table 6: To what extent would you agree with the following statements?