"Security issues should be addressed immediately regardless of who created it": Sysadmins' Security Vulnerability Ownership and Remediation Decisions

Tamara Bondar
Carleton University
TamaraBondar@cmail.carleton.ca

Hala Assal
Carleton University
Hala.Assal@carleton.ca

***Abstract*—System administrators are the ones primarily responsible for ensuring the security of their systems and services. While security is typically atop their considerations, they also tend to various competing priorities. Through an interview study with 7 sysadmins, and a large-scale survey study with 124 sysadmins in North America, this paper explores factors influencing system administrators' security vulnerability remediation decisions. In addition, we explore how the vulnerability creator (whether the sysadmin themself or another sysadmin) affects remediation decisions.**

Our findings reveal that remediation decisions are often complex and influenced by various factors, including vulnerability severity and the sysadmin's skills and experience. The creator of the vulnerability had minimal effect on vulnerability remediation decisions, as we found that sysadmins typically assume *psychological ownership* and moral responsibility towards their systems. Collaboration between sysadmins, and with third-party vendors was recommended by our participants to facilitate vulnerability remediation.

I. Introduction

Organizations are increasingly facing security threats due to vulnerabilities discovered on a daily basis. The year 2024 saw a 20% increase in the number of exploited vulnerabilities compared to the previous year [38]. This, coupled with the fact that almost a quarter of Common Exploited Vulnerabilities (KEVs) were exploited on or the day before their Common Vulnerabilities and Exposures (CVE) was publicized [38] is particularly concerning. Security threats affect organizations of varying sizes and industry sectors (*e.g.,* children smart device manufacturers [30], smart city devices [45], defence organizations [5]). Such threats could have implications on user data security and could extend to users' physical safety, and often lead to organizations' revenue loss. In 2024, data breaches cost an average of $4.88M globally [31].

As primary maintainers of information systems, system administrators (henceforth sysadmins) are (often solely) responsible for system security, including mitigating, and identifying and remediating vulnerabilities. These vulnerabilities can be introduced to the system through design issues or through vulnerable third-party systems (*e.g.,* third-party software libraries) [67]. To stay updated on new vulnerabilities, sysadmins can rely on community forums and blogs, and databases (*e.g.,* National Vulnerability Database (NVD) [47]). To monitor their systems, sysadmins also deploy network security tools (eg [74], [51]), and *incident response systems* to monitor for security incidents (*i.e.,* violations of the organization's security policies).

Once a vulnerability is detected in the system, the sysadmin has to engage in an elaborate process involving identifying affected systems, assessing the impact of the vulnerability, and designing and implementing appropriate remedies. The initial discovery or detection of the vulnerability is out of scope of this work, we focus on sysadmins' response after discovering a vulnerability, such as factors that could influence remediation decisions

Existing human-centric research about sysadmins has primarily focused on the initial discovery of vulnerabilities and approaches to inform sysadmins about new threats. The use of notifications is a common approach to inform sysadmins about vulnerabilities, *e.g.,* using WHOIS [16] domain records. This approach has been effective in increasing awareness of vulnerabilities, and in improving the rate of remediation particularly for high severity vulnerabilities [40], [23]. However, increasing awareness alone is not sufficient as sysadmins may still choose to ignore patching vulnerabilities [40], *e.g.,* due to compatibility issues [10].

In this paper, we investigates factors that could influence sysadmins' vulnerability remediation decisions. We also explore whether and how who the creator of the vulnerability is (*i.e.,* the entity who introduced the vulnerability to the system) affects remediation decisions. To this end, we pursue two research questions:

RQ1: What factors influence sysadmins' remediation decisions for different types of security vulnerabilities?

RQ2: How does the creator of a security vulnerability influence sysadmins' remediation decisions?

Through an interview study and a large scale survey study with sysadmins in North America, we show that sysadmins' vulnerability remediation decisions are often complex and

Symposium on Usable Security and Privacy (USEC) 2026
27 February 2026, San Diego, CA, USA
ISBN 978-1-970672-07-7
https://dx.doi.org/10.14722/usec.2026.23054
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

influenced by various factors, including the severity of the vulnerability and the sysadmin's level of technical skill. We found that sysadmins often bear the sole responsibility for many decisions, which can be burdensome and error-prone. When a vulnerability is discovered, sysadmins in our study expressed the need for collaboration and facilitated communication with other admins within their organization, as well as third-party vendors as applicable. Additionally, we found that our participants exhibited *psychological ownership* [50], [17] to *their* systems, thus the identity of the vulnerability creator (whether the sysadmin themself or another) had minimal effect on remediation decisions. We discuss this further in Sec. VI-B.

II. Background and Related Work

A. Background

Definition of vulnerabilities. There is no one universally accepted definition for vulnerabilities. Several definitions have been proposed by cybersecurity experts. The most pertinent to our research is that by Dowd *et al.* [22], defining vulnerabilities as: *"specific flaws or oversights in a piece of software that allow attackers to do something malicious - expose or alter sensitive information, disrupt or destroy a system, or take control of a computer system or program."*

Vulnerability taxonomies and classifications. Previous work emphasized the importance of standardized vulnerability classifications (*e.g.,* [32]). Seacord and Householder [54] note that without a commonly agreed-upon classifications, organizations use different approaches to vulnerability classification, making it difficult to compare vulnerabilities across systems or to correlate them with incidents, exploits and effective countermeasures. Aslam *et al.* [7] proposed a taxonomy of security faults to classify and analyze vulnerabilities in computer systems, to aid in the development of targeted solutions for common faults. Tsipenyuk *et al.* [65] presented a taxonomy of software security errors based on eight categories that represent common classes of software security flaws, including API abuse, security features, and encapsulation. However, without a universally-accepted standard, such classifications may not be adopted.

Vulnerabilities' severity ratings and databases. The Common Vulnerability Scoring Systems (CVSSs) [25] is a widely used rating system for security vulnerabilities, offering a score from 0 to 10 based on the potential impact of the vulnerability and exploitation complexity. It is employed by the National Institute of Standards and Technology (NIST) NVD [47], a government-funded database of vulnerability information accessible to the public. Another important resource is the Common Weakness Enumeration (CWE) [62], a community-developed list of software security weaknesses with its scoring system (the Common Weakness Scoring System (CWSS)), tailored for software vulnerabilities. The CWSS rates vulnerabilities based on their likelihood of being exploited, the impact of a successful exploit, and the difficulty of detecting and preventing an exploit.

Additionally, some organizations have developed their own rating systems. For example, Red Hat adopts a severity rating system [53] ranging from low to critical based on the potential impact and ease of exploiting the vulnerability. Additionally, Microsoft's Damage, Reproducibility, Exploitability, Affected Users, and Discoverability (DREAD) model [39] evaluates five factors, such as the potential damage from the vulnerability, how easily the vulnerability can be reproduced, and how many users would be affected if the vulnerability was exploited.

B. Related work

In this section, we discuss previous research focusing on sysadmins' security vulnerability management.

Vulnerability notification. Previous work [40], [23], [59], [21], [73] has investigated various methods to notify sysadmins of vulnerabilities within their systems. Notification methods varied in their modality (*e.g.,* emails [40], [21]), whom to contact [59], [40], and the language used (*e.g.,* English *vs.* the receiver's native language) [40], [73]. While notification campaigns generally motivated some sysadmins to address vulnerabilities in their system, these campaigns were not always successful. The decision to address a vulnerability was found to rely on different factors, in addition to vulnerability discovery (*e.g.,* through notifications) [58], [23].

Vulnerability management practices. Vulnerability Management refers to the proactive identification, evaluation, and remediation of vulnerabilities affecting systems within an organization. Sysadmins manage software updates to protect their systems against known vulnerabilities; however, this is often challenging due to lack of information on updates and the potential impact of deployment [41]. Sysadmins, even the most experienced, often have trouble predicting update outcomes, and are thus generally reluctant to applying them [64]. Often, sysadmins rely on informal channels (*e.g.,* blogs) and community support (*e.g.,* the *patchmanagement.org* mailing list) to deal with issues and updates, especially when an official patch is yet to be released [34]. However, managing and coordinating information from the myriad of information sources has led some to device their own "socio-technical resources" to address issues [35]. Furthermore, remediation practices tend to be complicated by competing priorities and resource limitations. In fact, even for high profile vulnerabilities, organizations may delay remediation when it negatively affects performance [46]. In addition, identifying relevant and affected parties [46] and the extensive coordination involved in vulnerability management [70], [19], [46] often results in long delays in applying security patches [20].

Dey *et al.* [18] argue that remediation policies would be more effective when informed by multiple metrics such as the severity level of vulnerabilities, patching cost, and expected disruptions to operations. Bondar *et al.* [10] identified factors that contribute to sysadmins' lack of remediation, despite knowledge of vulnerabilities. These included, backwards compatibility issues, lack of resources, the sysadmin's technical knowledge of the vulnerability, and internal company politics.

Challenges in vulnerability management. Vulnerability management tends to be a highly collaborative process that often involves IT specialists, managers, and internal and

external security experts [70], [19]. Sysadmins thus need to communicate and coordinate between the various teams and departments [56]. This was identified by previous work as one of the challenges in vulnerability management (whether through applying updates or patch management). Additionally, most organizations lack formal processes for updates and patch management [64], leaving sysadmins without formal guidance. However, sysadmins' confidence in their abilities and training varies [64], which can lead to an added strain on sysadmins. Other challenges include, the need for coordination between the various stakeholders who could have conflicting priorities [19], [56], lacking usability of security tools [19], complex IT environments [56], difficulty in identifying and prioritizing vulnerabilities [56], [57], managing legacy software that has reached the end of its support lifecycle [35], and the need for balanced security and operational requirements [56], [18]. Matters are complicated when vulnerable systems are used and operated by a different organization [37]. The organization using the system generally prefers to address the vulnerability in-house to minimize cost, however, they may lack the necessary technical expertise [37]. Recent work explored the use of ChatGPT [1] to support vulnerability management [44]. While promising, the study showed the importance of human verification of generated results.

III. Study design and methodology

We designed and conducted a preliminary interview study with sysadmins to gain insights on their experience with different types of vulnerabilities. Results from the interview study and our review of the literature informed our large-scale survey study. Both studies are approved by our IRB. On recruitment, we did not restrict participation by job title. Instead, we determined participant eligibility based on their typical job activities, *e.g.,* maintaining and configuring systems in their organizations. The advertised purpose of both studies was "to learn about your duties, priorities, and factors that influence your decisions."

A. Interview study

We advertised the study on sysadmin-focused social media groups. Interested participants filled out a prescreening survey on Qualtrics to ensure eligibility and a diverse sample. Eligible participants were then invited to the interview study, prior to which they completed a demographics questionnaire. The interview (Appendix B) covered sysadmins' knowledge of and previous experience with vulnerabilities, their experience in addressing misconfigurations, their decision-making factors, and organizational support. Interview sessions were audio-recorded and later transcribed for analysis. We used Trint [42] for transcription, and manually verified the transcripts for correctness and completeness. Before running the study, we pilot tested the interview with 2 sysadmins. Data from pilot testing is not included in the data analysis.

We selected and invited 10 participants, ensuring diversity in gender, age, job title. Seven participants responded to our invitation and completed the study. We did not invite more participants as we had reached data saturation [27] and no new insights were gained from further data collection. Interviews lasted 18-41mins (avg = 26min), and participants received a $25 CAD Amazon gift card as compensation. All interviews were conducted in September 2022.

To analyze the data, we employed the Thematic Analysis method [11]. Using NVivo [72], we assigned codes to describe valuable information conveyed in quotes. The one researcher who conducted all interviews performed the open coding to ensure analysis quality and that contextual insights are not missed [12]. Throughout this iterative process, to ensure analysis reliability and minimize researcher bias, the research team met regularly to discuss the codes, ensure no information is missed or misrepresented, and identify emerging themes. Our analysis resulted in 52 codes forming 10 themes. Appendix E shows an example of the identified themes and their codes.

B. Survey study

The survey (Appendix C) addressed 12 topics, including sysadmins' knowledge of and previous experience with vulnerabilities, their experience in addressing misconfigurations, their decision-making factors, organizational support, as well as the topics of third-party vulnerabilities and vulnerability prioritization.

The survey also included eligibility and attention check questions to ensure the quality of our data, as well as demographic questions. Eligibility questions included 2 technical questions from a beginner courses for system administrators [15] to test sysadmins' knowledge. Attention-check questions were placed at roughly equal intervals within the survey. We pilot tested the survey with 2 sysadmins prior to running the study. Data from pilot testing is not included in the data analysis. To avoid fatigue, we organized the survey into blocks based on the topics addressed, and allowed participants a 24-hour window to complete the survey. On average, the survey took 41 minutes to complete. Participants received $20 CAD as compensation.

In the first quarter of 2023, we recruited sysadmins employed in North America through Prolific [52] and concurrently from sysadmin-focused social media groups (*e.g.,* on LinkedIn [43]). The survey was hosted on Qualtrics [2] survey platform. We received 72 responses from Prolific and 702 from social media. The suspiciously high number of responses from social media was a result of a bot attack on our survey, despite our preemptive measures (*e.g.,* using reCaptcha and Qualtrics's built-in functionality).

To ensure data quality, we employed Qualtrics data quality filters and manually went over the data to remove suspicious submissions (*e.g.,* those containing gibberish, duplicate qualitative responses, and those with exact start and end times). After our diligent data-cleaning process, we had 50 valid responses from Prolific and 74 from social media. The results presented herein are from these 124 valid participants.

To analyze quantitative data, we used IBM SPSS Statistics $v.28$. Herein, we report the actual number of responses analyzed for each test, as participants had the ability to skip

questions. For within-subject tests, we used the Friedman Rank Sum Test [26], [48] for ordinal data or when normality was not assumed. When applicable, as a post-hoc analysis, we used Wilcoxon Signed-rank Test [71], [24] with Bonferroni corrections [69], [24]. For qualitative data, we used an iterative thematic analysis process to analyze responses to open-ended questions, and used it to corroborate or challenge the results of the statistical tests.

C. Ethical considerations

Both studies were reviewed and approved by our IRB. We did not collect any personally-identifying information and ensured participants' anonymity (*e.g.,* disabling IP location tracking on Qualtrics). Before each study, participants were provided with a consent form detailing the purpose of the study, our data storage and retention approach, procedure for withdrawal from the study, and the audio-recording and the use of Trint for transcription in the interview study. Aside from eligibility questions, participants could skip any question they were uncomfortable answering.

D. Limitations

Similar to other studies in the field, our data is self-reported and may be incomplete or influenced by biases. We employed different strategies to address this. For example, we ensured participants' anonymity in our study. Additionally, we added scenario-based questions to reduce social-desirability bias, used gender-neutral names to reduce gender biases, and randomized question order when possible to reduce order bias. As we could not verify participants' employment as sysadmins (as we did not request personal information), we verified participants' sysadmin knowledge by including technical questions in our survey. In addition, since participants self-select to participate in the studies, it is possible that they may have different characteristics or motivations than those who did not (*e.g.,* our participants may be more proactive towards vulnerability management). Additionally, all our participants are employed in North America, which may not necessarily reflect experiences world-wide.

IV. Interview Study Results

A. Participants' demographics ($n = 7$)

We interviewed 7 participants (2 women and 5 men), with age range 25–45 years. Participants were employed either full-time ($n = 5$), part-time ($n = 1$), or as a contractor ($n = 1$), with varying years of experience of at least 1-3 years. See Appendix D for full demographics information.

B. Vulnerability understanding

We found that participants had a mostly abstract understanding of vulnerabilities mostly revolving around data access. P2 explained, *"if my system is vulnerable, it means someone else other than me can get access to the information."* Our participants mainly considered vulnerabilities as weaknesses that are introduced to their organizations from external sources (n=5), and only two participants discussed misconfigurations.

C. Organizational processes

Work review: presence and influence. All participants but one have work reviews, albeit with varying degrees of formality. These range from scheduled and structured reviews to informal mentorship. In general, participants perceive a work review process to be valuable as it allows for the sharing of security expertise, discussions of potential or popular security issues, and building strategies to ensure their systems are secure. However, one participant explained that work reviews can cause stress and complicate the sysadmin's work process, especially when it involves unrealistic consequences. P1 explained, *"They always give me a little timeframe to improve, and that really puts me under pressure."*

Support and accountability. We found that in general participants received support from their organizations in the form of resources and equipment, as well as by allowing them extra time to solve security issues and hiring additional personnel if needed. All participants agreed that in case of a security breach, the responsible party must be identified. However, participants were divided on whom they would place the responsibility; some believed that it should always be the system's sysadmin, while others believed that the team leader should take responsibility.

D. Factors influencing sysadmins' remediation decisions

We found that the remediation decision-making process is always complex, requiring reviewing vulnerability and system information, and influenced by a combination of different factors (discussed below). The type of vulnerability (*i.e.,* third-party vulnerability *vs.* misconfiguration) is inconsequential to the decision. Participants generally engaged in a cost-benefit analysis process, however, we found that all costs seem to become negligible if the vulnerability's perceived negative impact on the system is significant.

Knowledge and experience. Participants identified security knowledge and direct experience identifying and fixing vulnerabilities as influential factors in determining whether/when to address vulnerabilities. Participants believed that experienced sysadmins would require less time to solve security issues. They also indicated that the first time a sysadmin addresses a specific vulnerability is more difficult than subsequent occurrences. On the other hand, those without proper experience could pose a risk to the company's reputation and status, and are more likely to leave known vulnerabilities unresolved. For example, P5 explains how lacking experience has led to a security incident in her organization, *"Well, what can we say is that the fault was [employee name]. It was as a result of ignorance or lack of experience [...] my idea is he really didn't know what he was doing."* As security is a fast-changing field, participants recognized that *continuous learning* is essential for sysadmins to keep up with the latest advancement in the field and ensure their knowledge and skills are up to date.

Fix complexity. Participants indicated that the complexity of the remediation process (*e.g.,* patch or applying a change in system settings or firewall) is another key deciding factor.

Complex fixes are unfavourable, *e.g.,* because these *"take more time [...] to be integrated into the system"* [P6]. Participants try to avoid such complex fixes by assessing the vulnerability more deeply to determine *"if the vulnerability is serious and whether it is worth spending much time and effort on it"* [P4].

Time constraints. The amount of time required to complete the remediation process was another influential factor identified by our participants. This factor is also dependent on the fix complexity, the sysadmin's experience, and vulnerability severity. For example, when lacking time, complex and low-severity vulnerabilities would be deferred. Participants indicated that rushing to complete a fix, due to lack of time, could inadvertently lead to creating additional issues.

Collaboration opportunities. Participants indicated that collaboration is an integral part of the daily work process of sysadmins. They identified the ability to receive support while addressing vulnerabilities from other experts in the field as an influential motivating factor for vulnerability remediation. Participants expressed that receiving support from more advanced colleagues could help resolve issues faster and more effectively, while also allowing them to get advice on improving the system and preventing further security problems.

E. Misconfigurations vs. Third-party vulnerabilities

Participants indicated that they would prioritize remediating third-party vulnerabilities over misconfigurations, as they perceived the risk from the former to be higher. Participants also referred to their organizations' policies to inform their decision, as these different types of vulnerabilities are addressed separately. P6 explained, *"if we're talking about the third-party vulnerability and then security misconfigurations, this will be classified on a different level of security to breach or security protocol."* In comparing difficulties addressing the different types of vulnerabilities, we found that participants considered that addressing third-party vulnerabilities would require more time and collaboration with other sysadmins within the organization. Participants also explained that addressing vulnerabilities that they do not typically manage or fixing a misconfiguration created by another sysadmin would require more cognitive effort. P5 explained, *"A system that I set up myself, I understand this system, and I also know I used best practices to set it up. As for a system that wasn't set up by me, I think it will actually take me longer."* This could be due to lack of understanding of the foreign system, exacerbated by lack of documentation or not following best practices. P7 noted, *"I've seen so many system administrators [who] are not using their programming skills. For their work, I have to spend a lot of time in the day to understand it."*

V. Survey Study Results

A. Participants' demographics

Herein, we report on the 124 valid responses to our online survey, unless otherwise stated.

Our participants are employed in organizations in the United States (63%) or Canada (37%). Gender distribution in our dataset aligns with industry statistics [13], [75], with 19.4% of participants identifying as women, and 80.6% as men. All participants had recent sysadmin work experience, with the majority having at least 3 years. Participation was not limited by job titles, rather based on job duties. The most common job titles reported by participants are: System Administrator, System engineer, IT Infrastructure Analyst, Network Administrator, and Database Engineer. See complete demographic information in Appendix D.

B. Vulnerability understanding

Security vulnerability in general. The majority of our participants (69.4%) have a clearer understanding of what a vulnerability is, compared to interview participants. For instance, P44 described it as: *"it typically means that an attacker has access to the system (to conduct malicious activity) due to a security weakness or through social engineering tactics."* Some participants, however, had simpler descriptions such as a *"system error"* [P55] or *"a bug in the program"* [P117]. We also explored participants' understanding of misconfigurations and third-party vulnerabilities.

Security misconfiguration. The majority of participants (66.1%) described a security misconfiguration as a mistake in the configuration of security settings in a computer system, network, or software application that makes it vulnerable to attacks. Participants explained that a system can be misconfigured due to the sysadmins' insufficient knowledge about security settings, incorrect configuration, or a failure to update settings in response to new threats. Participants also mentioned failure to install security patches, inadequate security policies, weak passwords, and excessive access rights as examples of security misconfiguration.

Third-party vulnerabilities. Participants generally described a third-party vulnerability as a security risk or weakness caused by a third-party provider or service, such as an external vendor or software provider. According to participants, this type of vulnerability may expose the organization's data or systems to malicious attacks. Participants also explained that such vulnerabilities can exit in hardware or software managed by a third-party that their organization uses.

C. Work setting and previous experience

The majority of participants (73%) indicated that their teams desire allocating more time towards security, whereas 85% indicated that their organizations allow enough time towards applying security updates. We now dig deeper into sysadmins' work procedures and previous vulnerability experience.

Work review. Approximately 90% of participants agreed that having a "work review" would be highly beneficial, and 81% believed that it could reduce the number of security vulnerabilities. Such a review would be similar to code reviews in software development where a colleague or supervisor double-checks their work. Half of our participants reported having such a review, however only 35% of participants reported having it on a regular basis and 6% of participants do not receive any reviews as they work independently. Some

participants (7%) also reported having access to a mentor for advice, but they do not review their work.

Company support. We asked participants about the type of support their companies provide to deal with security vulnerabilities. The majority of participants (77%) reported receiving necessary equipment, 60% receive additional resources for learning, almost 60% of participants have access to extra help and time for challenging tasks, and over half of the participants (66%) receive financial incentives. Only 2% of participants reported not receiving any type of support.

Experience with vulnerabilities overall. Almost 61% of participants deal with security vulnerabilities at least once a week. Half of our participants begin addressing the vulnerability within a few hours of its discovery, while 18% take a day, and 29% take from a few days to more than a week.

Experience with misconfigurations. The vast majority of our participants (72%) reported having prior experience in addressing security misconfigurations. These had varying degrees of impact, ranging from minor issues to major breaches, such as the exposure of personal data and system downtime resulting in revenue loss. Most participants (60%) faced misconfigurations resulting from other sysadmin(s)' work. Almost a third of our participants reported the need to put in extra effort beyond applying a fix due to their unfamiliarity with the history behind these misconfigurations. P1 explained that they first need to *"evaluate why the misconfiguration occurred and what it should have been in the first place."* We also found that participants generally exhibited hesitancy in making changes to other sysadmins' work without enough context. For example, P45 explained, *"I would first confirm with the manager if it was intentional, because I don't want to assume that it is a misconfiguration; it could be used for testing or other purposes. Once I assess that, I will ensure that it will not cause any impact and create a change management request so it is approved and documented."*

Experience with third-party vulnerabilities. Compared to misconfigurations, a smaller percentage of our participants experienced third-party vulnerabilities (42%). Our results show that participants mainly rely on the third-party provider to provide a software solution to address such vulnerabilities. For example, P16 explained, *"The vendor helped us properly patch the compromised system and remedy any security issues."* Others expected further involvement from the third-party providers, beyond a software solution, *e.g.,* P117 recalled, *"We've dealt with it several times before. We will first tell the company that provides this service and then ask them to send someone to help us deal with it."*

Perception of risk. Around half of our participants considered security misconfigurations to be less critical than third-party vulnerabilities. Their rationale is that system misconfigurations are less likely to be known to adversaries (unless it is a targeted attack), whereas third-party vulnerabilities are publicized. This explains why the majority of our participants (70%) would prioritize fixing a third-party vulnerability over a security misconfiguration in their systems.

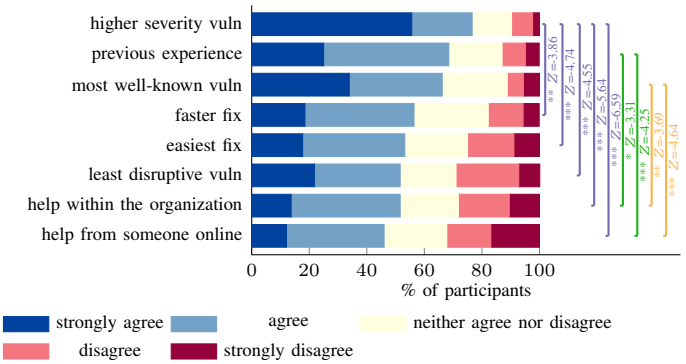

Fig. 1. Factors influencing security vulnerability remediation decisions. ($\chi^2(7) = 82.35, p < .001, N = 124$) ***: $p \leq .001$, **: $p < .01$, *: $p < .05$

D. Factors influencing sysadmins' prioritization of remediation decisions

Vulnerabilities overall To investigate factors that influence sysadmins' prioritization decisions when addressing vulnerabilities overall, we asked participants to rate their agreement with the following eight prompts, all starting with *"When I decide whether to fix a vulnerability, I prioritize..."*:

- based on the vulnerability severity, and fix the higher severity first - *[higher severity vuln]*
- the one that I had a previous experience with - *[previous experience]*
- the most well-known vulnerabilities - *[most well-known vuln]*
- the one that I can fix faster - *[faster fix]*
- the vulnerability with the least complicated fix - *[easiest fix]*
- the vulnerability that is least disruptive to my organization/clients - *[least disruptive vuln]*
- based on a chance to ask someone for help within my organization - *[help within the organization]*
- based on a chance to ask someone for help online (e.g., StackOverflow) - *[help from someone online]*

As shown in Fig. 1, the top three prioritization factors relate to security risk and the sysadmins' experience. Our results show that participants would prioritize addressing *higher severity vulns*, vulnerabilities with which they had *previous experience*, and the *most well-known* vulnerabilities.

Our statistical analysis shows that these prioritization factors vary significantly. Post-hoc analysis shows that participants are significantly more likely to prioritize the vulnerability with higher severity regardless of its disruptive impact on the organization or the fix's characteristics; they would prioritize it over the vulnerability with a faster fix, the least disruptive vulnerability, or the vulnerability with the easiest fix. Participants are also more likely to prioritize the higher severity vulnerability regardless of whether they have help from someone within the organization or from someone online.

On the other hand, participants' previous experience with a vulnerability is a significantly more influential prioritization factor compared to being able to get help from colleagues,

or online. Similarly, the most well-known vulnerability would significantly be prioritized over being able to get help from within the organization, or online.

Misconfiguration Factors. We asked participants to rate 18 factors according to their importance when deciding to fix security misconfigurations specifically (see Q26 in Appendix C). These factors were identified as potentially influential in previous research, such as:

- My skills/experience - *[skills/experience]*
- Severity of the misconfiguration - *[misconfiguration severity]*
- Who created the security misconfiguration - *[misconfig creator]*

The top two most important factors (Fig. 2) were the *sysadmins' skills and experience* and the *severity of the misconfiguration*, aligning with influential factors for vulnerabilities overall (discussed above).

We found that these factors vary significantly in their influence on sysadmins' decisions when addressing misconfigurations. Participants' skills/experience with the misconfiguration is significantly more influential than the fix's *time expectations*, the *time available* for remediation, who the *misconfiguration creator* is, whether participants can have their *fix double-checked*, if they have *weekly meetings* with colleagues, or participants' degree of *job satisfaction*. We also found that the *misconfiguration severity* is significantly more influential in participants' decision to prioritize remediation, regardless of who *misconfiguration creator* is, or whether they have *weekly meetings* with colleagues.

Third-party factors Focusing on factors that could influence remediation decisions of third-party vulnerabilities, we compiled a list of 18 factors informed by our review of the literature and our interview study results. Participants were asked to rate the importance of each factor in their decision-making process (see Q34 in Appendix C). These factors included:

- Severity of the third-party vulnerability - *[3rd party severity]*
- The potential impact of the third-party vulnerability on my system - *[impact on the system]*
- Patch complexity/characteristics - *[patch complexity]*

As shown in Fig. 3, the top two most influential decision factors were *3rd party severity* and the potential *impact on the system*. The Sysadmins' *skills/experience* remains one of the top 3 factors, similar to misconfigurations.

These 18 factors vary significantly in their influence on sysadmins' third-party remediation decisions. Our analysis showed that *3rd party severity* is significantly more influential in participants' decisions than the availability of support and resources, such as receiving *help from experienced sysadmin*, having access to *extra learning* opportunities or *forums and groups*, and having *weekly meetings*. The third-party vulnerability's *impact on the system* was more significant than participants' *job satisfaction*, and whether they have *weekly meetings*. We also found that participants' *skills/experience* was a more significant influencer compared to having *weekly meetings*.

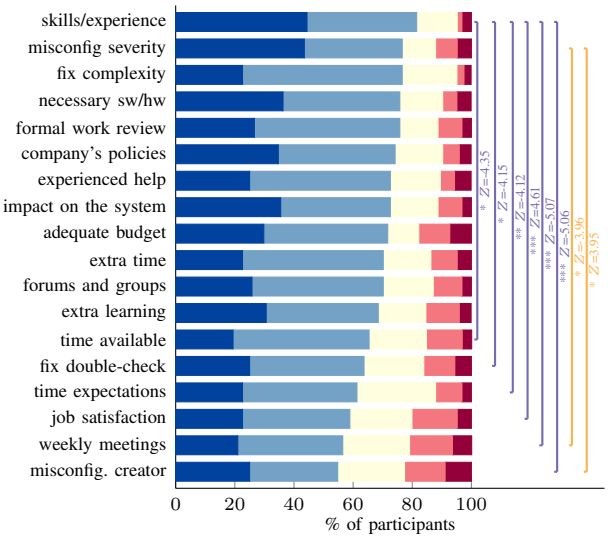

Fig. 2. Factors influencing security misconfiguration remediation decisions. ($\chi^2(17) = 86.24, p < .001, N = 124$) ***: $p \leq .001$, **: $p < .01$, *: $p < .05$)

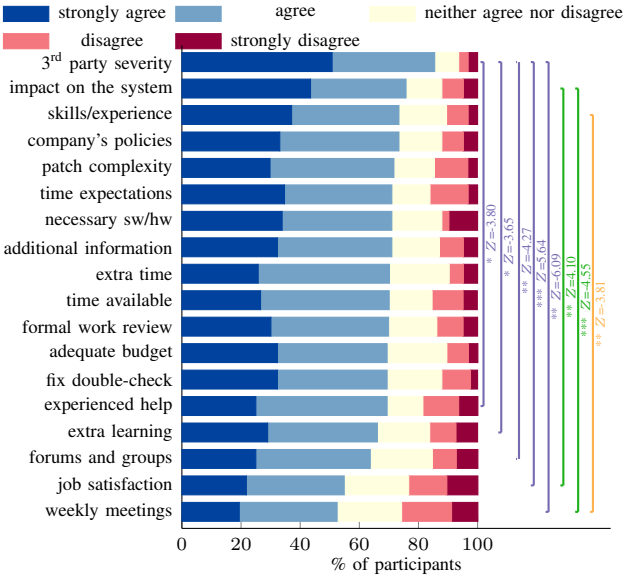

Fig. 3. Factors influencing third-party vulnerability remediation decisions. ($\chi^2(17) = 82.44, p < 0.001, N = 123$) ***: $p \leq .001$, **: $p < .01$, *: $p < .05$

This highlights how participants care about minimizing negative impacts of third-party vulnerabilities on their systems, and it also shows how sysadmins' technical competencies plays an important role in third-party remediation decisions.

E. Exploring factors across organizations and industry sectors

Here we explore whether the importance of prioritization factors varies depending on the organization's size or industry sector. To investigate, we first divided the participants into two categories based on their organization's size [66]: SMEs with up to 500 employees and LEs with 500+ employees. We also grouped participants based on their organization's

industry sector, into IT Service providers, IT enterprises, Non-IT Enterprises, and Government services.

*1) **Misconfiguration Factors**:* We performed the Friedman test within each group to examine if the significance of the 18 misconfiguration factors varied based on the size of the organization or industry sector. When significant, we performed post-hoc analysis using Wilcoxon test with Bonferroni correction.

- ***Organization size.*** We found that the factors differed significantly within SMEs ($\chi^2(17) = 57.74, p < .001, N = 95$) and within LEs ($\chi^2(17) = 63.2, p < .001, N = 28$). Post hoc analysis revealed that for SMEs, the sysadmins' *skills/experience* is significantly more important than having *extra time* ($Z = -2.86, p = .034$), *fix time duration* ($Z = -2.86, p = .034$), having someone to *double-check the fix* ($Z = -3.1, p = .01$), having an *adequate budget* ($Z = -3.1, p = .009$), the admins' *job satisfaction* level ($Z = 3.1, p = .009$), the *misconfiguration creator* ($Z = -3.2, p = .007$), the *time available* to apply the fix ($Z = -3.2, p = .005$), and having *weekly meetings* ($Z = -3.3, p = .004$). This highlights the importance of sysadmins' technical competency in SMEs, especially over time and budget constraints when fixing misconfigurations. On the other hand, participants from LEs valued the *company's policies* significantly more than having *weekly meetings* ($Z = -5.4, p = .022$) and who *misconfiguration creator* is ($Z = 6.1, p = .003$). The *misconfiguration creator* was also significantly less important than having *necessary software/hardware* ($Z = 5.6, p = .012$), the misconfiguration's *impact on the system* ($Z = 5.39, p = .024$), and having an *adequate budget* ($Z = 5.16, p = .046$).
- ***Industry sector.*** Friedman test for the Government services group was not significant ($\chi^2(17) = 18.46, p = .36, N = 10$). It was significant for the IT Service providers ($\chi^2(17) = 30.56, p = .023, N = 50$) and the Non-IT enterprises ($\chi^2(17) = 34.59, p = .007, N = 19$), yet post hoc analyses were not significant. Misconfiguration factors varied significantly for IT Enterprises ($\chi^2(17) = 40.13, p = .001, N = 43$); having *necessary software/hardware* was significantly more important than whom the *misconfiguration creator* is ($Z = 4.24, p = .035$).

*2) **Third-party factors**:* Similar to misconfigurations, we explored whether the 18 third-party factors vary in their importance based on organization size or industry sector.

- ***Organization size.*** Factors differed significantly within SMEs ($\chi^2(17) = 53.46, p < .001, N = 94$) and within LEs ($\chi^2(17) = 48.28, p < .001, N = 28$). Post-hoc analysis showed that for SME participants, *3rd party severity* is significantly more important than their *job satisfaction* ($Z = 3.36, p = .02$) or having *weekly meetings* ($Z = -4.005, p < .001$). The *impact on the system* is also more important than having *weekly meetings* ($Z = -2.97, p = .021$). For LEs, *3rd party vulnerability severity* was significantly more important than participants' *job satisfaction* ($Z = 5.29, p = .032$).
- ***Industry sector.*** Friedman test was not significant for the Government services group ($\chi^2(17) = 17.405, p = .427, N = 10$). It was significant for the IT Service providers ($\chi^2(17) = 29.33, p = .032, N = 49$), yet post-hoc analysis was not significant. We found that factors varied significantly for the IT Enterprise group ($\chi^2(17) = 40.19, p = .001, N = 43$) and the Non-IT Enterprise group ($\chi^2(17) = 30.73, p = .022, N = 19$). Post-hoc analysis showed that *3rd party vulnerability severity* was significantly more important than *weekly meetings* for both the IT Enterprise group ($Z = -4.7, p = .007$) and the Non-IT Enterprise group ($Z = -6.34, p = .038$).

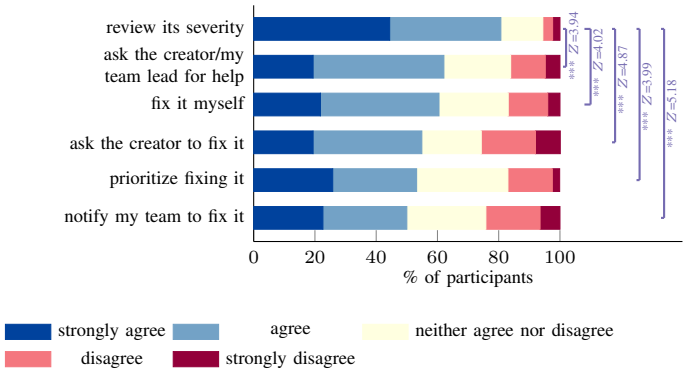

Fig. 4. Strategies for addressing a security misconfiguration in an inherited system. ($\chi^2(5) = 43.01, p < .001, N = 124$). ***: $p \leq .001$

F. Who is responsible for remediating security vulnerabilities?

The vast majority of participants (75%) reported that having support from colleagues when dealing with vulnerabilities is valuable, and most (59%) indicated that such support increases the likelihood of them fixing the vulnerability. While some participants (47%) indicated that the creator of a misconfiguration should be the one to fix it, 75% of our participants expressed willingness to collaborate on remediation efforts regardless of who created the vulnerability. Participants highlighted the importance of remediating vulnerabilities, *e.g.,* P27 said, *"we don't care who fixes a problem, as long as it gets done fast"*.

To explore whether the creator of the vulnerability influences remediation decisions, we asked participants to rate different strategies when addressing a misconfiguration in their system that was created by another sysadmin (Q.21 in Appendix C). The top three strategies (Fig. 4) were reviewing the misconfiguration severity, requesting support from the sysadmin who created the misconfiguration or their own team leader, and attempting to remediate the misconfiguration themselves. Reviewing the misconfiguration severity was statistically the most significant strategy compared to all others.

To further explore participants' opinions of whom should assume the responsibility of fixing vulnerabilities and to avoid social desirability bias, we created four scenarios: two for misconfigurations and two for third-party vulnerabilities (Q.24-25, 32-33 in Appendix C). In the scenarios, a vulnerability

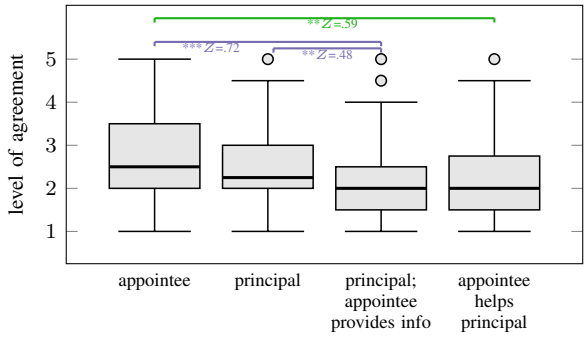

Fig. 5. Agreement to whom should fix a misconfiguration in both scenarios: $(\chi^2(3) = 28.47, p < .001, N = 124)$. **: $p < .01$, ***: $p \leq .001$ (1: strongly agree)

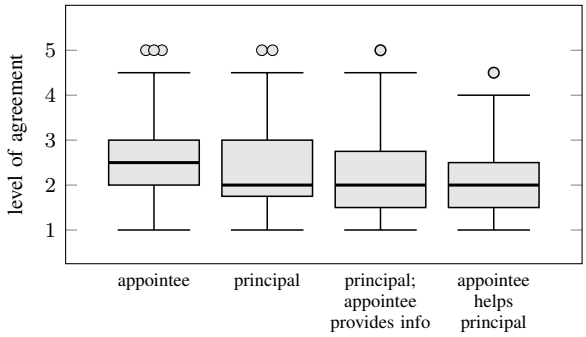

Fig. 6. Median agreement to whom should fix a vulnerability in both third party scenarios: $(\chi^2(3) = 10.27, p = .02, N = 124)$. Post-hoc analysis was not significant. (1: strongly agree)

is created by an *appointee* sysadmin: a sysadmin who was temporarily managing the system or one who has moved later away from this role. The current and ongoing sysadmin (henceforth, *principal* sysadmin) discovers the vulnerability after the appointee had moved on. Through Likert-scale questions, participants indicated whom they thought should fix the discovered vulnerability. All scenarios used gender-neutral names to avoid gender stereotypes. Fig. 5 and Fig. 6 show the median scores and statistical tests for the two misconfiguration and third-party vulnerability scenarios, respectively.

Misconfigurations. Participants generally appreciated the risks associated with vulnerable systems. P16 explained, *"security issues should be addressed immediately regardless of who created it."* When addressing the discovered security misconfigurations, participants favoured collaboration between the principal and appointee sysadmins. Approaches with only one of the sysadmins (principal or appointee) addressing a misconfiguration were significantly less favoured by participants than having the principal sysadmin address it while the appointee provides contextual information if needed. The appointee sysadmin addressing the misconfiguration alone was also significantly less favoured than the appointee collaboratively addressing the misconfiguration with the principal sysadmin. Participants considered collaborative efforts an opportunity for improvement and to ensure that *"they don't make the same mistake again"* [P48]. And while some participants thought that fairness indicates that the admin who created the misconfiguration (*i.e.,* the appointee sysadmin) should be the one to fix it, they recognized the logistical infeasibility since *"[it is] not technically their responsibility anymore"* [P41].

Third-party vulnerabilities. Post-hoc statistical analysis did not show significant differences between approaches. However, our analysis shows that participants generally favoured collaborative approaches between the principal and appointee sysadmins to address the third-party vulnerability, or that the principal sysadmin would fix it alone. We found that participants generally did not place the burden of the remediation on the appointee, and some proposed to *"contact the [third-party] vendor"* [P12] for support and information.

G. Challenges in system administration and future outlook

Ending our survey, we asked participants to share their thoughts about their sysadmin experiences. Most interestingly, participants reflected on challenges they face, *e.g.,* managing legacy systems and lacking budget and resources. P16 explained, *"While there are many tools that allow us to manage our system updates [...], our organization also has to maintain legacy systems that run customized applications, so these are very tricky since their OS is very outdated [or updates...] are no longer available!"* Participants described their field as continuously evolving, and that sysadmins *"need to have a growth mindset"* [P48], however lacking resources often force sysadmin to be *"reactive"* [P30]. One participant had an optimistic outlook to the future, P18 said, *"[...] as more companies move towards containerization/Kubernetes, there will be fewer configuration mistakes, and software updates and fixes will be easier and quicker to implement."*

VI. Discussion

A. Answering RQ1: Factors influencing remediation decisions

The remediation decision process is complex and is dependent on different, often competing, factors. Our results show that sysadmins generally prioritize addressing higher severity vulnerabilities. They are concerned more about negative consequences of third-party vulnerabilities as these are typically publicly known, in contrast to misconfigurations. When addressing the latter, the sysadmin's skill level and prior experience addressing misconfigurations becomes a top influential factor, more than when dealing with third-party vulnerabilities. This could be because a misconfiguration is typically unique to the system, and the sysadmin (often solely) diagnoses the issue, identifies possible solutions, and implements the solution that ensures security while minimizing disruptions. Whereas, when addressing third-party vulnerabilities, sysadmins can rely on available patches/updates, and third-party vendor and community support.

Work review and documentation. In software development, code reviews contribute to ensuring code security [63] and present an in-context opportunity for learning and knowledge transfer [8]. Our participants generally valued having

their work reviewed by colleagues or a manager, yet the majority did not have a formal work review procedure in place. Such reviews can help ensure security, and can also be an opportunity to discuss identified vulnerabilities, assess their risk, and plan to avoid them in the future. When addressing misconfigurations specifically, sysadmins often need to gather contextual information about the misconfiguration (*e.g.,* its severity, what was initially intended) before designing and applying a solution. The quality of this procedure is thus highly dependent on the sysadmin's skills and experience. Formal work review and proper documentation can aid in ensuring that decisions are recorded for future clarifications if needed, and that sysadmins follow proper procedures and protocols. We do, however, stress the importance of providing sysadmins with necessary resources and sufficient time to address these vulnerabilities, to avoid stress and employee burnout. Further research is needed to devise methodologies to support the seamless integration of formal reviews and documentation production within sysadmins' workflow.

Influential factors for SMEs *vs.* LEs. SMEs typically have limited resources, budget, and a limited IT staff, often with limited security expertise [55]. Additionally, sysadmins in SMEs often assume multiple roles due to limited resources and staffing [4]. Thus, in such organizations, the sysadmin's skills and experience can be critical when addressing vulnerabilities. On the other hand, LEs often have complex and legacy systems, as well as regulatory compliance requirements [33], [60]. Tiefeneau *et al.* [64] found that most organizations do not have formal processes, and that sysadmins in SMEs do not feel as confident in their training as those in LEs. This highlights the importance of formalized procedures for mitigating and managing security risks [68], [36]. With such clear guidance, sysadmins, in SMEs and LEs alike, can rely on established policies to guide their actions, as opposed to relying solely on their own experience or intuition.

B. Answering RQ2: Effect of vulnerability creator

Interestingly, the perceived creator of a vulnerability differs between misconfigurations and third-party vulnerabilities. In the case of misconfigurations, sysadmins in our study perceived the sysadmin responsible for the incorrect setup as the creator, whereas for third-party vulnerabilities, the vendor—not the sysadmin who installed the software—is considered the creator. However, in both cases, this had minimal to no effect on remediation decisions.

Sysadmins in our study exhibited *psychological ownership* [50], [17] of their systems. They considered the principal sysadmin as the *owner* of the system who assumed the moral obligation, in addition to their work responsibility, to maintain system security. This was true regardless of how long the principal sysadmin had assumed this role, *i.e.,* even in cases when the sysadmin recently inherited a vulnerable system, it became the principal's moral duty to address the vulnerability in *their* system. In the case of misconfigurations, collaboration between the principal sysadmin and the misconfiguration creator was expected and recommended. The purpose of the collaboration is to provide the principal sysadmin with contextual information to aid in remediating the misconfiguration, and the creator with awareness of the issue to avoid its reoccurrence. In the case of third-party vulnerabilities, participants expected support (*e.g.,* in the form of patches) and collaboration with third-party vendors when needed.

Psychological ownership has been shown to produce positive outcomes, *e.g.,* increased motivation, increased investment in skill improvement, and job satisfaction [50]. However, with competing factors and limited resources, sysadmins often need to rely on the support of their peers and their community, especially to properly and efficiently assess vulnerability severity [6], [70], [29]. Future research should explore methods to promote collaboration between sysadmins and to facilitate information flow. This could include devising secure methods allowing temporary system access to sysadmins beyond the principal sysadmin to allow for collaboration during vulnerability remediation.

C. Reflections

Almost two decades ago the research community recognized the need for human-centric approaches even for technical users [14]. While the research community has paid special attention to developer-centric research [49], [61], human-centric research focusing on sysadmins is generally lacking [9], [3]. Our study shows that sysadmins are often left to deal with vulnerabilities without proper support (*e.g.,* adequate resources, senior mentors), while grappling with different priorities [10]. Sysadmins often have to rely on, and coordinate between, a myriad of tools and information sources which can place a substantial cognitive load on them [9]. Additionally, without a formal processes to follow, many decisions are left solely to the sysadmin's discretion, including risk assessment, time allocation, and prioritization. These decisions can thus be error prone, inconsistent across time or across different sysadmins, and also depend heavily on the sysadmin's skills and experience. Our results highlight the need for more systematic processes (*e.g.,* work review) that introduce a level of formalization to decisions, without conflicting with sysadmins' workflow. For example, a Service Level Agreement (SLA) is a formal agreement between customer and a service provider defining various aspects, such as the services to be provided, standards for performance, and the responsibilities of both sides [28]. Future research can explore how such a concept can be applied within organizations to specify sysadmins' duties and responsibilities as well as the organization's responsibility towards supporting its sysadmins (*e.g.,* resources, learning opportunities, clear paths for collaboration between sysadmins).

VII. Conclusion

We conducted an interview study, and a large-scale survey study with 124 system administrators employed in North America to explore sysadmins' decision-making process regarding vulnerability remediation, as well as the effect of the vulnerability creator on remediation decisions. We found that remediation decisions are influenced by various factors,

most importantly the vulnerability severity and the sysadmin's technical skills and experience. The creator of the vulnerability had minimal effect on remediation decisions. Interestingly, we found that sysadmins exhibit *psychological ownership* to their systems, as they assume the moral responsibility to maintain system security regardless of who created the vulnerability. Collaboration between sysadmins, and with third-party vendors, was recommended by our participants to address security vulnerabilities. We discussed future research directions aiming to support sysadmins' remediation decision-making processes, as well as to encourage collaboration and information sharing.

REFERENCES

[1] ChatGPT. https://chatgpt.com. Last accessed on 30.03.2025.

[2] Qualtrics. https://www.qualtrics.com.

[3] SOUPS 2024: Reflecting on Twenty Years of Usable Privacy and Security. https://www.youtube.com/watch?v=_GWGWhdsRdU. Last accessed on 18.03.2023.

[4] The IT Skills Gap: Jack of All Trades, Master of None. https://bitwizards.com/blog/the-it-skills-gap, Dec 2021.

[5] Hussain Ahmad, Isuru Dharmadasa, Faheem Ullah, and Muhammad Ali Babar. A review on c3i systems' security: Vulnerabilities, attacks, and countermeasures. *ACM Computing Surveys*, 55(9):1–38, 2023.

[6] Noura Alomar, Primal Wijesekera, Edward Qiu, and Serge Egelman. " you've got your nice list of bugs, now what?" vulnerability discovery and management processes in the wild. In *Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security*, pages 319–339, 2560 Ninth St. Suite 215 Berkeley, CA, United States, 2020. USENIX Association.

[7] Taimur Aslam, Ivan Krsul, and Eugene H Spafford. Use of a taxonomy of security faults. *Department of Computer Science Technical Reports. Paper 1305.*, 1996.

[8] Alberto Bacchelli and Christian Bird. Expectations, outcomes, and challenges of modern code review. In *2013 35th International Conference on Software Engineering (ICSE)*, pages 712–721, 2013.

[9] Rob Barrett, Eser Kandogan, Paul P Maglio, Eben M Haber, Leila A Takayama, and Madhu Prabaker. Field studies of computer system administrators: analysis of system management tools and practices. In *Proceedings of the 2004 ACM conference on Computer supported cooperative work*, pages 388–395, 2004.

[10] Tamara Bondar, Hala Assal, and AbdelRahman Abdou. Why do internet devices remain vulnerable? a survey with system administrators. In *Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb 2023)*. NDSS, 2023.

[11] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006.

[12] Virginia Braun and Victoria Clarke. One size fits all? what counts as quality practice in (reflexive) thematic analysis? *Qualitative Research in Psychology*, 18(3):328–352, 2021.

[13] Employment Canada and Social Development. Network system administrator in ontario: Job prospects - job bank. https://www.jobbank.gc.ca/marketreport/outlook-occupation/3751/ON, Feb 2023. Last accessed on 30.03.2023.

[14] Sonia Chiasson, PC van Oorschot, and Robert Biddle. Even experts deserve usable security: Design guidelines for security management systems. In *SOUPS Workshop on Usable IT Security Management (USM)*, pages 1–4, 2007.

[15] Coursera. System administration and it infrastructure services. https://www.coursera.org/learn/system-administration-it-infrastructure-services/home/info. Last accessed on 18.03.2023.

[16] Leslie Daigle. RFC 3912: WHOIS Protocol Specification. https://datatracker.ietf.org/doc/html/rfc3912, 2004.

[17] Sarah Dawkins, Amy Wei Tian, Alexander Newman, and Angela Martin. Psychological ownership: A review and research agenda. *Journal of Organizational Behavior*, 38(2):163–183, 2017.

[18] Debabrata Dey, Atanu Lahiri, and Guoying Zhang. Optimal policies for security patch management. *INFORMS Journal on Computing*, 27(3):462–477, 2015.

[19] Nesara Dissanayake, Asangi Jayatilaka, Mansooreh Zahedi, and M Ali Babar. Software security patch management-a systematic literature review of challenges, approaches, tools and practices. *Information and Software Technology*, 144:106771, 2022.

[20] Nesara Dissanayake, Mansooreh Zahedi, Asangi Jayatilaka, and Muhammad Ali Babar. Why, how and where of delays in software security patch management: An empirical investigation in the healthcare sector. *Proc. ACM Hum.-Comput. Interact.*, 6, November 2022.

[21] Adam Doupé, Bryce Boe, Christopher Kruegel, and Giovanni Vigna. Fear the EAR: discovering and mitigating execution after redirect vulnerabilities. In *ACM Conference on Computer and Communications Security (CCS)*, 2011.

[22] Mark Dowd, John McDonald, and Justin Schuh. *The art of software security assessment: Identifying and preventing software vulnerabilities*. Pearson Education, 2006.

[23] Zakir Durumeric, Frank Li, James Kasten, Johanna Amann, Jethro Beekman, Mathias Payer, Nicolas Weaver, David Adrian, Vern Paxson, Michael Bailey, et al. The matter of heartbleed. In *Proceedings of the 2014 conference on internet measurement conference*, pages 475–488, 2014.

[24] Andy Field. *Discovering statistics using IBM SPSS statistics*. sage, 2013.

[25] Forum of Incident Response and Security Teams, Inc. Common vulnerability scoring system sig. https://www.first.org/cvss/. Last accessed on 30.03.2023.

[26] Milton Friedman. The use of ranks to avoid the assumption of normality implicit in the analysis of variance. *Journal of the American statistical association*, 32(200):675–701, 1937.

[27] Barney G Glaser and Anselm L Strauss. *Discovery of grounded theory: Strategies for qualitative research*. Routledge, 2017.

[28] Jahyun Goo. Structure of service level agreements (sla) in it outsourcing: The construct and its measurement. *Information Systems Frontiers*, 12:185–205, 2010.

[29] Julie M Haney and Celeste Lyn Paul. Toward integrated tactical operations for red/blue cyber defense teams. In *Workshop on Security Information Workers at Symposium on Usable Privacy and Security*, 2018.

[30] MA Hannan Bin Azhar, Danny Smith, and Aimee Cain. Spying on kids' smart devices: Beware of security vulnerabilities! In *Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability, London, September 2022*, pages 123–140. Springer, 2023.

[31] IBM. Cost of a data breach report 2024. https://www.ibm.com/reports/data-breach.

[32] Vinay M Igure and Ronald D Williams. Taxonomies of attacks and vulnerabilities in computer systems. *IEEE Communications Surveys & Tutorials*, 10(1):6–19, 2008.

[33] Daehee Jang and Heesun Yun. Effective memory diversification in legacy systems. *International journal of electrical and computer engineering systems*, 14(3):321–331, 2023.

[34] Adam Jenkins, Pieris Kalligeros, Kami Vaniea, and Maria K. Wolters. "anyone else seeing this error?": Community, system administrators, and patch information. In *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 105–119, 2020.

[35] Adam D G Jenkins, Linsen Liu, Maria K Wolters, and Kami Vaniea. Not as easy as just update: Survey of system administrators and patching behaviours. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI '24, New York, NY, USA, 2024. Association for Computing Machinery.

[36] David Kluge and Samuel Sambasivam. Formal information security standards in german medium enterprises. In *CONISAR: The Conference on Information Systems Applied Research*, 2008.

[37] Lorenz Kustosch, Carlos Gañán, Michel van Eeten, and Simon Parkin. Patching up: Stakeholder experiences of security updates for connected medical devices. In *34th USENIX Security Symposium (USENIX Security 25)*, pages 2265–2281, 2025.

[38] Ravie Lakshmanan. 768 cves exploited in 2024, reflecting a 20% increase from 639 in 2023. https://thehackernews.com/2025/02/768-cves-exploited-in-2024-reflecting.html.

[39] David LeBlanc. Dreadful. https://learn.microsoft.com/en-us/archive/blogs/david_leblanc/dreadful, Aug 2007. Last accessed on 30.03.2023.

[40] Frank Li, Zakir Durumeric, Jakub Czyz, Mohammad Karami, Michael Bailey, Damon McCoy, Stefan Savage, and Vern Paxson. You've got

vulnerability: Exploring effective vulnerability notifications. In *USENIX Security Symposium*, volume 16, 2016.
[41] Frank Li, Lisa Rogers, Arunesh Mathur, Nathan Malkin, and Marshini Chetty. Keepers of the Machines: Examining How System Administrators Manage Software Updates For Multiple Machines. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 273–288, Santa Clara, CA, August 2019. USENIX Association.
[42] Trint Limited. Transcribe video and audio to text: Content editor. https://trint.com/. Last accessed on 18.03.2023.
[43] LinkedIn. Welcome to your professional community. https://www.linkedin.com/home. Last accessed on 30.03.2023.
[44] Peiyu Liu, Junming Liu, Lirong Fu, Kangjie Lu, Yifan Xia, Xuhong Zhang, Wenzhi Chen, Haiqin Weng, Shouling Ji, and Wenhai Wang. Exploring ChatGPT's capabilities on vulnerability management. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 811–828, Philadelphia, PA, August 2024. USENIX Association.
[45] Ben Lupton, Mackenzie Zappe, Jay Thom, Shamik Sengupta, and Dave Feil-Seifer. Analysis and prevention of security vulnerabilities in a smart city. In *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0702–0708. IEEE, 2022.
[46] Gerbrand ten Napel, Michel van Eeten, and Simon Parkin. Speedrunning the maze: Meeting regulatory patching deadlines in a large enterprise environment. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 504–521, 2025.
[47] NIST. National vulnerability database. https://nvd.nist.gov/. Last accessed on 30.03.2023.
[48] Marija J Norušis. *SPSS 14.0 guide to data analysis*. Prentice Hall Upper Saddle River, NJ, 2006.
[49] Olgierd Pieczul, Simon Foley, and Mary Ellen Zurko. Developer-centered security and the symmetry of ignorance. In *Proceedings of the 2017 New Security Paradigms Workshop*, pages 46–56, 2017.
[50] Jon L Pierce, Tatiana Kostova, and Kurt T Dirks. Toward a theory of psychological ownership in organizations. *Academy of management review*, 26(2):298–310, 2001.
[51] Joseph A Plot. Red team in a box (rtib): Developing automated tools to identify, assess, and expose cybersecurity vulnerabilities in department of the navy systems. Technical report, NAVAL POSTGRADUATE SCHOOL MONTEREY CA, 2019.
[52] Prolific. Prolific: quickly find research participants you can trust. https://www.prolific.co/, 2014. Last accessed on 18.03.2023.
[53] Red Hat. Understanding red hat security ratings. https://access.redhat.com/security/updates/classification. Last accessed on 30.03.2023.
[54] Robert C Seacord and Allen D Householder. A structured approach to classifying security vulnerabilities. Technical report, CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2005.
[55] Alireza Shojaifar and Heini Järvinen. Classifying smes for approaching cybersecurity competence and awareness. In *Proceedings of the 16th International Conference on Availability, Reliability and Security*, ARES '21, New York, NY, USA, 2021. Association for Computing Machinery.
[56] Murugiah Souppaya, Karen Scarfone, et al. Guide to enterprise patch management technologies. *NIST Special Publication*, 800:40, 2013.
[57] Jessica Staddon and Noelle Easterday. "it's a generally exhausting field" a large-scale study of security incident management workflows and pain points. In *2019 17th International Conference on Privacy, Security and Trust (PST)*, pages 1–12. IEEE, 2019.
[58] Ben Stock, Giancarlo Pellegrino, Frank Li, Michael Backes, and Christian Rossow. Didn't you hear me?–Towards more successful Web vulnerability notifications. In *Network and Distributed System Security (NDSS)*, 2018.
[59] Ben Stock, Giancarlo Pellegrino, Christian Rossow, Martin Johns, and Michael Backes. Hey, you have a problem: On the feasibility of large-scale web vulnerability notification. In *USENIX Security Symposium*, 2016.
[60] Kristan Stoddart. Gaining access: Attack and defense methods and legacy systems. In *Cyberwarfare: Threats to Critical Infrastructure*, pages 227–280. Springer, 2022.
[61] Mohammad Tahaei and Kami Vaniea. A survey on developer-centred security. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 129–138. IEEE, 2019.
[62] The MITRE Corporation. Common weakness enumeration. Last accessed on 30.03.2023.
[63] Christopher Thompson and David Wagner. A large-scale study of modern code review and security in open source projects. In *Proceedings of the 13th International Conference on Predictive Models and Data Analytics in Software Engineering*, PROMISE, pages 83–92, New York, NY, USA, 2017. Association for Computing Machinery.
[64] Christian Tiefenau, Maximilian Häring, Katharina Krombholz, and Emanuel von Zezschwitz. Security, availability, and multiple information sources: Exploring update behavior of system administrators. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 239–258. USENIX Association, August 2020.
[65] Katrina Tsipenyuk, Brian Chess, and Gary McGraw. Seven pernicious kingdoms: A taxonomy of software security errors. *IEEE Security & Privacy*, 3(6):81–84, 2005.
[66] US Small Business Administration. What's new with small business? https://www.sba.gov/sites/default/files/Whats_New_With_Small_Business.pdf, 2016. Online; last accessed on January 19, 2023.
[67] Paul C van Oorschot. *Computer Security and the Internet*. Springer, 2020.
[68] Jinx P Walton. Developing an enterprise information security policy. In *Proceedings of the 30th annual ACM SIGUCCS conference on User services*, pages 153–156, 2002.
[69] Eric W Weisstein. Bonferroni correction. *https://mathworld. wolfram. com/*, 2004.
[70] Rodrigo Werlinger, Kasia Muldner, Kirstie Hawkey, and Konstantin Beznosov. Preparation, detection, and analysis: the diagnostic work of it security incident response. *Information Management & Computer Security*, 18(1):26–42, 2010.
[71] Frank Wilcoxon. Individual comparisons by ranking methods. biometrics bulletin; 1 (6): 80–83. *International Biometric Society, Wiley, US*, 1945.
[72] LP Wong. Data analysis in qualitative research: A brief guide to using nvivo. *Malaysian family physician: the official journal of the Academy of Family Physicians of Malaysia*, 3(1):14, 2008.
[73] Eric Zeng, Frank Li, Emily Stark, Adrienne Porter Felt, and Parisa Tabriz. Fixing https misconfigurations at scale: An experiment with security notifications. In *The 2019 Workshop on the Economics of Information Security (2019)*, 2019.
[74] Yu Zhang, Wei Huo, Kunpeng Jian, Ji Shi, Haoliang Lu, Longquan Liu, Chen Wang, Dandan Sun, Chao Zhang, and Baoxu Liu. Srfuzzer: an automatic fuzzing framework for physical soho router devices to discover multi-type vulnerabilities. In *Proceedings of the 35th annual computer security applications conference*, pages 544–556, 2019.
[75] Zippia, Inc. Computer systems administrator demographics and statistics [2023]: Number of computer systems administrators in the us. https://www.zippia.com/computer-systems-administrator-jobs/demographics/, Sep 2022. Last accessed on 30.03.2023.

APPENDIX

A. Interview demographics survey

1) What is your age range?
   a) 18-24
   b) 25-31
   c) 32-38
   d) 39-45
   e) Other. Please specify:
   f) Prefer not to say
2) What is the highest level of education you have completed?
   a) Some school
   b) High school
   c) College Degree
   d) Bachelor's Degree
   e) Master's Degree
   f) Ph.D.
   g) Other. Please specify:
   h) Prefer not to say
3) To which industry sector does your organization belong?
4) How big is your team?
   a) Just me

b) 2 to 10 people
c) 11 to 20 people
d) 21+
e) I don't know
f) Prefer not to say

5) How would you rate your security experience on a scale of 1 (novice) to 5 (proficient)?
6) How would you rate your system administration expertise on a scale of 1 (novice) to 5 (proficient)?
7) How often do you attend Sysadmin conferences/events?
a) Once a year
b) A few times a year
c) Every month
d) I have never attended before, but plan to attend this year
e) I have never attended before, and do not plan to attend
f) Other. Please specify:
g) Prefer not to say

B. Interview script

Previous experience

1) Can you describe your daily tasks and work processes?
2) How did you acquire the knowledge necessary for your job? (e.g., through formal education, courses, certification)
3) Do you have a direct supervisor?
4) Do you have employees under your supervision?

General questions about vulnerabilities

1) What do you consider a vulnerability? Please try to give a specific definition. Provide definition: *Vulnerabilities are specific system characteristics exploited by attacks, including design flaws, implementation flaws, and deployment or configuration issues (e.g., lack of physical isolation, ongoing use of known default passwords, debugging interfaces left enabled).* This is how the term "vulnerability" was defined in the book "Computer Security and the Internet: Tools and Jewels" by Paul C. van Oorschot.
2) Have you ever faced security vulnerabilities? Which types? How often do you deal with them?
3) What factors do you consider when you decide about fixing security vulnerabilities?
4) Does [factor] can influence the decision about fixing the vulnerability?
   - Patch complexity/characteristics
   - Administrator's skills/experience
   - Collaboration issues
   - Time-consuming fixes
   - Severity of the vulnerability
5) How long does it usually take to start to fix the security vulnerability?
6) What are your first steps after you find out that there is a vulnerability in your system?
7) What kinds of issues do you typically face when trying to fix security vulnerabilities?

Experience with misconfigurations

1) Would you say that your system has ever had a security misconfiguration?
2) Can you elaborate on who was involved and how it was remediated if applicable? Remind: Remember that you should not give me any names; please focus mostly on job titles, how they are a part of your team, whether they are a part of a different team and so on.
3) Have you ever found a misconfiguration made by someone else?
4) What factors do you consider when making a decision about fixing a misconfiguration?
5) Are these considerations the same when you were setting up the system vs when someone else was setting it up?
6) Do you need to do any additional steps or processes if the system was set up by someone else?

Factors influencing their decision-making process

1) Is there any difference in the factors considered when deciding about fixing a misconfiguration and third-party vulnerability?
2) What factors would you consider when deciding which vulnerability to fix first?

Support from the organization

1) Does your company provide any support when dealing with security issues?
2) Does the company give you enough time for security issues and security protection?
3) Let's imagine that a vulnerability was found in the system, and this vulnerability led to a data leak. Who would be responsible? How would your company react?
4) Do you face any issues when you are trying to do system upgrades or staff like that for security purposes (from the company perspective)? Do they provide you with enough time to keep system upgrades up to date?
5) Do you have any kind of review or evaluation included in your work process? Is anyone else reviewing your work?
6) In your opinion, how useful would a "work review" for system administrators (an analogue to the "code review" for developers) be?
7) If "work review" is implemented, how do you think it will influence your work process? And do you think it will decrease the number of security vulnerabilities?

Final

1) From your perspective, what recommendations do you have for improving the security-related work processes for system administrators? Any suggestions for companies' policies?
2) How do you enjoy doing your job?
3) Do you plan to change the area of your job in the next 2-3 years?
4) Is there anything you want to elaborate on? Or do you need any clarification? Please feel free to share your thoughts and concerns.

C. Online survey

Note: Text in this colour was not shown to participants.

1) Informed Consent Form [If "I do not consent", the survey ended showing participants' an ineligibility message]
   a) I consent
   b) I do not consent
2) [Prolific] What is your Prolific ID? Please note that this response should auto-fill with the correct ID.
3) [Social Media] Before you proceed to the survey, please complete the captcha below. [reCaptcha question]
4) Where is your organization located? If it is a branch of a larger organization, enter the country of the branch you are working in. [If not Canada or USA, the survey ended showing participants' ineligibility message]
   a) Canada
   b) USA
   c) Other
5) Please select the statement that best describes your primary job. [If not system administrator, the survey ended showing participants' ineligibility message]
   a) System administrator, system engineer, network administrator, etc.
   b) System designer, system developer, system engineer, etc.
   c) Web master, software developer, tester, etc.
   d) Other
6) In the past 3 years, how long have you been working in the system administration? [If less than 1, the survey ended showing participants' ineligibility message]
   a) Less than a year
   b) 1 year
   c) 2 years
   d) 3 years
7) Please consider the given scenario and choose the correct option.
   A particular computer on your network is a member of several GPOs. GPO-A has precedence set to 1. GPO-2 has a precedence set to 2, and GPO-C has a precedence set to 3. According to the given levels of precedence, what will be the resultant set of policy (RSOP) for this machine? [If not GPO-A, the survey ended showing participants' ineligibility message]
   a) The computer will default to local policy due to confusion.
   b) GPO-A will take precedence and overwrite any conflicting settings.
   c) GPO-B will take precedence and overwrite any conflicting settings.
   d) GPO-C will take precedence and overwrite any conflicting settings.
8) Please consider the given scenario and choose the correct option.
   Employees of a company are facing lots of bounced email notifications from email addresses they have never sent messages to. [If not DKIM method, the survey ended showing participants' ineligibility message]
   a) Mailboxes of the company users are full, resulting in bounced emails.
   b) SMTP would prevent such incidents as emails can be sent reliably using it.
   c) Having more than one email server would reduce such email bouncing incidents.
   d) An email authentication method like DKIM can be used to prevent such incidents.
9) What does it mean that a system has a "vulnerability"? Please explain what the term "vulnerability" means in your words.
10) For the rest of the survey, when we mention "vulnerability", we refer to it as defined below.
    Vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
    Examples of the vulnerabilities: buffer overflows, cross-site scripting, faulty or missing authentication, faulty firewall configurations, etc.
11) Please indicate that you have read the definition by choosing the correct answer. The *vulnerability* is:
    a) the property of non-public information remaining accessible only to authorized parties, whether stores (at rest) or in transit (in motion)
    b) a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source
    c) a set of computer programs and associated documentation and data
12) How often do you deal with vulnerabilities in your work?
    a) Daily
    b) A few times a week
    c) Once a week
    d) A few times a month
    e) Once a month
    f) I do not deal with vulnerabilities
13) On average, how long does it usually take to start to fix the security vulnerability?
    a) A few hours
    b) A day
    c) A few days
    d) A week
    e) Longer than a week
14) What do you consider a security "misconfiguration"? Please give a definition in your words.
15) For the rest of the survey, when we mention "misconfiguration", we refer to it as defined below.
    Misconfiguration is an incorrect or suboptimal configuration of an information system or system component that may lead to vulnerabilities (bad or publicly known passwords, faulty or missing authentication, faulty firewall configuration, missing encryption, faulty storage configuration, deployment of revealing information, etc.).
16) Please indicate that you have read the definition by choosing the correct answer. The *security misconfiguration* is:
    a) the technical activity of estimating risk or simply identifying threats of major concern, and the business

activity of "managing" the risk, i.e., making an informed response.
   b) is the process of monitoring and analyzing system events to identify and report an event on a host or network that violates security policy.
   c) an incorrect or suboptimal configuration of an information system or system component that may lead to vulnerabilities.
17) Have you ever dealt (e.g., identifying and/or remediating) with security misconfigurations in your systems?
   a) Yes
   b) No
18) [if Q17 is "Yes"] Please provide more details on what the impact of the security misconfiguration was, how it was resolved, and who was involved in fixing it (please do not include names, rather, focus on the position of those who was involved in fixing).
19) Have you ever had to deal with a security misconfiguration made by someone else?
   a) Yes
   b) No
   c) I don't know
20) Do you need to do any additional steps or processes before/when you start fixing the security misconfiguration if the system was configured by someone else?
   a) Yes. Please elaborate:
   b) No
   c) I haven't had to deal with this scenario before
   d) I don't know
21) Please rate your agreement with the following statements: *If I inherit a system with security misconfiguration(s) made by someone else...* [5-point Likert-scale: Strongly agree - Strongly disagree]
   a) I will ask that person to fix it
   b) I will fix it myself
   c) I will ask that person or my team leader to help me to fix it
   d) I will notify my team and let them deal with it
   e) I will prioritize fixing this issue above any other issue
   f) I will review the severity of this issue
   g) It will take me more time to fix it
   h) It will take me more effort to fix it
22) Please indicate your agreement with the statements provided below [5-point Likert-scale: Strongly agree - Strongly disagree]
   a) The misconfiguration should always be fixed by the employee who created it in the first place.
   b) I will never decline a chance to collaborate with my colleagues when I need to fix a security misconfiguration, regardless of who caused it.
23) What colour is grass? The fresh, uncut grass, not leaves or hay. We use this question as attention check, please make sure to select purple. [Attention check]
   a) Green
   b) Purple
   c) White
   d) Prefer not to say
24) Consider the following scenario and rate your agreement with the following statements. [5-point Likert-scale: Strongly agree - Strongly disagree]
   Sammie and Casey work as system administrators in different departments in the same company. While Casey was on vacation, Sammie was administering Casey's system and accidentally misconfigured it such that it made the system vulnerable. Once Casey returned from vacation, Casey discovered the issue; however, Sammie had returned to their usual duties in the other department by then. Who should fix this security misconfiguration?
   a) Sammie should fix it, as they created it
   b) Casey should fix it, as it is their responsibility, and they know the system well
   c) Casey should fix it, but should ask Sammie for details
   d) Sammie should help Casey to fix it
   e) It will be fair if Casey fixes the security misconfiguration
   f) It will be fair if Sammie fixes the security misconfiguration
   g) It will be fair if Sammie helps Casey fix the security misconfiguration
   h) Other thoughts? Please specify:
25) Consider the following scenario and rate your agreement with the following statements. [5-point Likert-scale: Strongly agree - Strongly disagree]
   Billie is a new system administrator in company X. Billie is taking Addison's place, as Addison has been promoted and moved to another department. Billie finds the misconfiguration in the system that they've just inherited from Addison. Who should fix this security misconfiguration?
   a) Addison should fix it, as they created it
   b) Billie should fix it, as now it is their responsibility
   c) Billie should fix it, but Billie should ask Addison for details of what Addison did
   d) Addison should help Billie to fix it, as Billie is new to the system and do not know all details yet
   e) It will be fair if Billie fixes the misconfiguration
   f) It will be fair if Addison fixes the misconfiguration
   g) It will be fair if Addison helps Billie to fix the misconfiguration
   h) Other thoughts? Please specify:
26) For each of the following factors, please rate their importance when deciding to fix a security misconfiguration. [5-point Likert-scale: Strongly agree - Strongly disagree]
   a) My skills/experience - *[skills/experience]*
   b) Severity of the misconfiguration - *[misconfiguration severity]*
   c) Fix complexity/characteristics - *[fix complexity]*
   d) Support from the organization by providing necessary software/hardware - *[necessary software/hardware]*
   e) Having a formal work review process - *[formal work review]*
   f) Company's policies (e.g., protocols) regarding to how and when to fix the security misconfiguration after it's

identification - *[company's policies]*

g) Support from the organization by providing access to another system administrator who has experience in the area - *[help from experienced sysadmin]*
h) The potential impact of the security misconfiguration on my system - *[impact on the system]*
i) Support from the organization by providing an adequate budget - *[adequate budget]*
j) Support from the organization by providing extra time - *[extra time]*
k) Having access to forums and sys admin groups - *[forums and groups]*
l) Support from the organization by providing extra learning opportunities (courses or certifications) - *[extra learning]*
m) The amount of time I have to work on the remediation process - *[time available]*
n) Having someone who can double-check my fix - *[fix double-check]*
o) How long I expect the remediation process to take - *[time expectations]*
p) The fulfilment and satisfaction received from my job - *[job satisfaction]*
q) Having weekly meetings with my colleagues - *[weekly meetings]*
r) Who has created the security misconfiguration - *[misconfiguration creator]*

27) What do you consider a "third-party vulnerability"? Please give a definition in your words.
28) For the rest of the survey, when we mention "third-party vulnerability", we refer to it as defined below.
Third-party vulnerabilities are vulnerabilities resulting from having relationships with external entities (service providers, integrators, vendors, telecommunications, and infrastructure support that are external to the organization that operates the manufacturing system).
29) Please indicate that you have read the definition, by choosing the correct answer. *The third-party vulnerability* is:
a) a vulnerability resulting from having relationships with external entities
b) a set of computer programs and associated documentation and data.
c) a series of steps, often implemented in software programs or hardware
30) Have you ever dealt with third-party vulnerabilities in your systems?
a) Yes
b) No
31) [If Q30 is "Yes"] Please provide more details on what the impact of the third-party vulnerability was, how it was resolved, and who was involved in fixing it (please do not include names, rather, focus on the position of those who was involved in fixing).
32) Consider the following scenario and rate your agreement with the following statements. [5-point Likert-scale: Strongly agree - Strongly disagree]
Ali and Brooks work as system administrators in different departments in the same company. While Brooks was attending a 7-day conference for system administrators, Ali was administering Brooks's system. Once Brooks returned from vacation, Brooks discovered the security third-party vulnerability in their system; however, Ali had returned to their usual duties in the other department by then. Who should fix this third-party vulnerability?
a) Ali should fix it, as the vulnerability appeared when Ali was on duty
b) Brooks should fix it, as it is their responsibility, and they know the system well
c) Brooks should fix it, but should ask Ali for details
d) Ali should help Brooks to fix it
e) It will be fair if Brooks fixes this third-party vulnerability
f) It will be fair if Ali fixes this third-party vulnerability
g) It will be fair if Ali helps Brooks fix this third-party vulnerability
h) Other thoughts? Please specify:
33) Consider the following scenario and rate your agreement with the following statements. [5-point Likert-scale: Strongly agree - Strongly disagree]
Morgan is a new system administrator in company X. Morgan is taking Jo's place, as Jo is going to retire in a few weeks. Morgan finds a third-party vulnerability in the system that they've just inherited from Jo. Jo is still going to work full-time for the next few weeks to finish the paperwork and help Morgan learn the system. Who should fix this third-party vulnerability?
a) Jo should fix it, as the vulnerability appeared when Jo was on duty
b) Morgan should fix it, as now it is their responsibility
c) Morgan should fix it, but Morgan should ask Jo for details of what happened
d) Jo should help Morgan to fix it, as Morgan is new to the system and do not know all details yet
e) It will be fair if Morgan fixes the misconfiguration
f) It will be fair if Jo fixes the misconfiguration
g) It will be fair if Jo helps Morgan to fix the misconfiguration
h) Other thoughts? Please specify:
34) For each of the following factors, please rate their importance when deciding to fix a security third-party vulnerability. [5-point Likert-scale: Strongly agree - Strongly disagree]
a) Severity of the third-party vulnerability - *[3rd party severity]*
b) The potential impact of the third-party vulnerability on my system - *[impact on the system]*
c) My skills/experience - *[skills/exeperience]*
d) Company's policies (e.g., protocols) regarding to how and when to fix the third-party vulnerability after its identification - *[company's policies]*
e) Patch complexity/characteristics - *[patch complexity]*

f) How long I expect the remediation process to take - *[time expectation]*
g) Support from the organization by providing necessary software/hardware - *[necessary software/hardware]*
h) Availability of additional information about the third-party vulnerability from the external sources - *[additional information]*
i) Support from the organization by providing extra time - *[extra time]*
j) The amount of time I have to work on the remediation process - *[time available]*
k) Having a formal work review process - *[formal work review]*
l) Support from the organization by providing an adequate budget - *[adequate budget]*
m) Having someone to double-check my fix - *[fix double-check]*
n) Support from the organization by providing access to another system administrator who has experience in the area - *[help from experienced sysadmin]*
o) Support from the organization by providing extra learning opportunities (courses or certifications) - *[extra learning]*
p) Access to forums and sys admin groups - *[forums and groups]*
q) The fulfilment and satisfaction received from my job - *[job satisfaction]*
r) Having weekly meetings with my colleagues - *[weekly meetings]*

35) Recall: We define vulnerability as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Please answer the following questions considering this definition.
36) What factors would you consider when deciding which vulnerability to fix first? How do you prioritize different vulnerabilities? Please complete the sentence and indicate how much you agree or disagree with each statement. *"When I decide whether to fix a vulnerability, I prioritize . . . "* [5-point Likert-scale: Strongly agree - Strongly disagree]
    a) based on the vulnerability severity, and fix the higher severity first
    b) the one that I can fix faster
    c) the one that I had a previous experience with
    d) the vulnerability with the least complicated fix
    e) the vulnerability that is least disruptive to my organization/clients
    f) the most well-known vulnerabilities
    g) based on a chance to ask someone for help online (e.g., StackOverflow)
    h) based on a chance to ask someone for help within my organization
37) Consider the following scenario and answer the question. Kim works as a system administrator. One day, doing regular system check-ups, Kim discovered 2 vulnerabilities in the system. The first one was critical with a complex fix, and the other one was not critical and easy to fix. Assuming that time is not an issue, which vulnerability should Kim fix first?
    a) The critical vulnerability with complex fix
    b) Not critical one with easy fix
38) Please indicate your agreement with the statements provided below [5-point Likert-scale: Strongly agree - Strongly disagree]
    a) My team would prefer to dedicate more time on security than what we currently do to prevent security vulnerabilities.
    b) It is easier to prevent a vulnerability than to fix it.
    c) It is cheaper to prevent a vulnerability than to fix it.
    d) Collaboration helps save time when dealing with vulnerabilities.
    e) I always follow the organization's security protocols when deciding about fixing vulnerabilities.
    f) Please choose "Strongly Agree" here [Attention check 2]
    g) Having a way to connect with my colleagues online and reach them in short term gives me a feeling of support when I start fixing vulnerabilities.
    h) I will be more likely to fix the vulnerability if I know that someone is there to help me in case something goes wrong.
39) Please indicate your agreement with the statements provided below [5-point Likert-scale: Strongly agree - Strongly disagree]
    a) Misconfigurations have less priority than third-party vulnerabilities, because only I can know about them.
    b) Third-party vulnerabilities become easily known, so they must be fixed with a higher priority.
40) Does your company give you enough time for searching for and dealing with security issues?
    a) Yes
    b) No
41) Does your company provide you with enough time to keep system upgrades up to date?
    a) Yes
    b) No
42) Please indicate your agreement with the statements provided below [5-point Likert-scale: Strongly agree - Strongly disagree]
    a) I often face issues when installing the security upgrades in my system.
    b) The main issue that stops me from installing security updates is that it usually takes much longer than expected.
    c) Company security policies prevent me from installing security updates.
    d) It takes a lot of effort and time to inform all employees about the system security updates, so some updates might be skipped.
43) Please choose ways your company supports you as a system administrator (choose all that apply to you).

a) Additional help
b) Financial motivation
c) Additional resources to study
d) Providing necessary equipment
e) More time for challenging tasks
f) Something else. Please specify:
g) My company does not provide me with any kind of support

44) Please indicate your agreement with the statements provided below [5-point Likert-scale: Strongly agree - Strongly disagree]
a) It's important to find the person who is responsible for the creation of vulnerability to prevent them from repeating this mistake.
b) The team lead should always be the one to take blame for the consequences of the attack on the vulnerability.

45) Do you have any kind of review or evaluation included in your work process?
a) Yes, my supervisor is reviewing my work
b) Yes, my colleague, who is on the same level as me, is reviewing my work
c) Yes, we have daily/weekly meetings with a team
d) Yes, I have a mentor, but they do not review my work
e) No, I work on my own

46) In your opinion, is it possible to implement a "work review" for system administrators (an analogue to the "code review" for developers)?
a) Yes, and it's already implemented
b) Yes, it is possible to implement
c) No, it is not possible

47) In your opinion, how useful would a "work review" for system administrators (an analogue to the "code review" for developers) be?
a) Extremely useful
b) Very useful
c) Moderately useful
d) Slightly useful
e) Not at all useful

48) If "work review" is implemented, do you think it will decrease the number of security vulnerabilities?
a) Yes
b) No

49) How do you enjoy doing your job?
a) Extremely
b) Very
c) Moderately
d) Slightly
e) Not at all

50) What is your current job title?

51) How many years of experience do you have in system administration?
a) 1 - 3 years
b) 4 - 10 years
c) 11+ years

52) How did you acquire the knowledge necessary for your job?
a) Self-taught
b) Formal education (college or university degree)
c) Online courses
d) Industry or on-the-job training
e) Through acquiring certification. Please give examples:
f) Other. Please specify:

53) What is your type of employment?
a) Contractor
b) Full-time employee
c) Part-time employee
d) Self-employed
e) Other. Please specify:

54) To which industry sector does your organization belong?
a) IT Service Provider (such as internet, network, storage, application as a service)
b) IT Enterprise (e.g., software company)
c) Non-IT Enterprise (core business other than IT)
d) Government/Public Services
e) Other. Please specify:

55) What is the approximate number of employees in your organization?
a) 1 - 10
b) 11 - 49
c) 50 - 249
d) 250 - 500
e) 501 or more
f) I don't know

56) How big is your team?
a) Just me
b) 2 to 10 people
c) 11 to 20 people
d) 21+
e) I don't know

57) How would you rate your following skills on a scale of 1 (novice) to 5 (proficient)? [5-point scale: 1-Novice to 5:Proficient]
a) Security experience
b) System administration expertise

58) How often do you attend sysadmin conferences/events?
a) Every month
b) A few times a year
c) Once a year
d) I have never attended before, but plan to attend this year
e) I have never attended before, and do not plan to attend
f) Other. Please specify:
g) Prefer not to say

59) Please indicate your agreement with the statements provided below [5-point Likert-scale: Strongly agree - Strongly disagree]
a) When choosing software to work with, I prefer to stick with software from an established, trusted company.
b) My level of caution and attentiveness when installing new software does not vary regardless of whether I have used it before or not.

60) Which gender identity do you identify with?

a) Woman
b) Man
c) Non-binary
d) Gender-fluid
e) Trans man
f) Trans woman
g) Two-spirit
h) I don't identify with any of the provided options. Please specify:

61) What is your age range?
a) 18 - 24
b) 25 - 31
c) 32 - 38
d) 39 - 45
e) Other. Please specify:

62) What is the highest level of education you have completed?
a) Some school
b) High school
c) College Degree
d) Bachelor's Degree
e) Master's Degree
f) Ph.D.
g) Other. Please specify:

63) Are there any factors that we hadn't considered? Is there anything you want to elaborate on? Please feel free to share your thoughts, ideas and concerns here. Please make sure not to include any personal information or information which may give away your identity.

64) Please enter your email address which we can use to send you the Amazon gift card as compensation for participation.

65) [If Q64 is skipped] We only use your email address to provide you with compensation. We do not have any other way to contact you. Please provide your email address.
a) My email address:
b) I recognize there is no other way to contact me. I do not want to provide my email address.

D. Demographics information

TABLE I
INTERVIEW PARTICIPANT DEMOGRAPHICS ($n = 7$)

P#	Job Title	Industry sector	Company size	Team size	Sec. exp.	Sysadmin exp.	Gender	Age	Country	Education	Years of Experience	Employment
P1	System engineer & database admin	Education	501+	21+	4	4	M	32-38	USA	Bachelor	11+	Full-time
P2	Computer Network admin	Health	250-500	21+	4	4	M	25-31	USA	Bachelor	4-10	Full-time
P3	admin	Marketing	11-49	11-20	4	4	M	25-31	CAN	Bachelor	1-3	Part-time
P4	System admin	Project Management	250-500	11 -20	3	3	W	25-31	CAN	Bachelor	1-3	Full-time
P5	System admin	IT	50-249	2-10	3	4	W	25-31	CAN	Bachelor	4-10	Contractor
P6	System & Network admin	Financial	50-249	11-20	4	4	M	25-31	USA	Bachelor	4-10	Full-time
P7	Networking & cybersecurity admin	Health	11-49	21+	5	4	M	39-45	CAN	PhD	4-10	Full-time

admin: administrator;
Sec experience: participants' self-reported security experience based on a scale 1(Novice) to 5(Proficient);
Gender: F: female, M: male

TABLE II: Survey participant demographics ($n = 124$)

PARTICIPANT		
Gender		
	Woman	19.4% ($n = 24$)
	Man	80.6% ($n = 100$)
Country		
	Canada	37% ($n = 46$)
	USA	63% ($n = 78$)
Age range		
	18 - 24	6.5% ($n = 8$)
	25 - 31	43.5% ($n = 54$)
	32 - 38	28.2% ($n = 35$)
	39 - 45	12.1% ($n = 15$)
	46+	9.7% ($n = 12$)
Experience (years)		
	1 - 3 years	32.3% ($n = 40$)
	4 - 10 years	49.2% ($n = 61$)
	11+ years	18.5% ($n = 23$)
Security experience self-rating[1]		
		$M = 3.85$
		$Md = 4$
System administration expertise[1]		
		$M = 4.15$
		$Md = 4$
Level of education completed		
	High school	5.6% ($n = 7$)
	College Degree	12.1% ($n = 15$)
	Bachelor's Degree	52.4% ($n = 65$)
	Masters Degree	25.0% ($n = 31$)
	Ph.D.	4.8% ($n = 6$)
Additional education[2]		
	Self-taught	28.2% ($n = 35$)
	Formal education	74.2% ($n = 92$)
	Online courses	44.4% ($n = 55$)
	Industry training	62.9% ($n = 78$)
Type of employment		
	Contractor	4.0% ($n = 5$)
	Full-time employee	84.7% ($n = 105$)
	Part-time employee	8.9% ($n = 11$)
	Self-employed	2.4% ($n = 3$)
Sysadmin conference attendance[3]		
	Every month	15 (12.1%)
	A few times a year	50 (40.3%)
	Once a year	32 (25.8%)
	Plan to attend this year	12 (9.7%)
	Do not plan to attend	11 (8.9%)
	Other	2 (1.6%)
Team		
Team size		
	Just me	2.4% ($n = 3$)
	2 to 10 people	63.7% ($n = 79$)
	11 to 20 people	29.0% ($n = 36$)
	21+	4.0% ($n = 5$)
	I don't know	0.8% ($n = 1$)
ORGANIZATION		
Number of employees		
	1 - 10	4.0% ($n = 5$)
	11 - 49	17.7% ($n = 22$)
	50 - 249	37.9% ($n = 47$)
	250 - 500	16.9% ($n = 21$)
	501 or more	22.6% ($n = 28$)
	I don't know	0.8% ($n = 1$)
Industry sector		
	IT Service Provider	40.3% ($n = 50$)
	IT enterprise	34.7% ($n = 43$)
	Non-IT Enterprise	15.3% ($n = 19$)
	Government/Public Services	9.7% ($n = 12$)

[1]Based on a scale from 1(Novice) to 5(Proficient); 1 participant decided not to provide this information.
[2]Participants could choose more than one option for additional education.
[3]2 participants skipped this question

E. Interview study qualitative data analysis

TABLE III
EXCERPT FROM INTERVIEW CODEBOOK

Code	Example Quote
Theme: Factors influencing remediation of vulnerabilities overall	
Previous experience	*"Administrators with lots of experience can actually fix vulnerabilities, ... issues a lot faster and in a more dynamic way."*
Finance resources	*"If managing a vulnerability for a particular organization, it has to do with a cost,* financially, *with available time for a fix, and with what the organization can afford."*
Available time	*"I think time is very important. Time management is something the system administrator should consider because when you're fixing these vulnerabilities, you have to be focused. So, I think* lack of time *is something that, you know, they have to look into."*
Patch complexity	"Complexity *would also affect the overall development of your system. If* a patch is complex*, it takes more time for these patches to be integrated into the system."*
Vulnerability severity	"Severity of the vulnerability *also influence the decision, you would take a different time factor."*
Theme: Difference in factors influencing remediation	
Misconfigs vs. Third-party vulnerabilities	*"In fixing misconfiguration, you pay more attention to* changing configurations*. And looking at a third-party vulnerability, you pay more attention to* service delivery, long-term importance and long-term efficiency*."*
Misconfigs vs Other vulnerabilities	*"I would say, there is* no difference*. It's likely the same thing."*
Own vs someone else's misconfigs	*"When someone else is setting up the system, it's going to be different depending on how they go about it, depending on how they set it. People have different ways of doing different things, so the configuration issues are not going to be the same."*
Theme: Work review	
Informal reviews	*"For us, it's our superior, the one that I'm under. I think he offers advice, supervises and also oversees most of what I'm doing."*
Reviews cause stress	*"That really puts me under pressure. So, I think that without evolution, it should be a little bit easier for me."*
Reviews are necessary	*"That would definitely reduce the number of security issues we had."*
Benefits of work reviews	*"They are asking for feedback on everything, and I've been like giving them honest feedback on what they've done. That's a great thing."*