Not as easy as just update: Survey of System Administrators and Patching Behaviours

Adam Jenkins
King's College London
London, England
adam.jenkins@kcl.ac.uk

Linsen Liu
University of Edinburgh
Edinburgh, Scotland
treellser@gmail.com

Maria Wolters
Society Division, OFFIS
Oldenburg, Germany
maria.wolters@offis.de

Kami Vaniea
University of Waterloo
Waterloo, Canada
kami.vaniea@uwaterloo.ca

ABSTRACT

Patching software theoretically leads to improvements including security critical changes, but it can also lead to new issues. For System Administrators (sysadmins) new issues can negatively impact operations at their organization. While mitigation options like test environments exist, little is known about their prevalence or how contextual factors like size of organization impact the practice of Patch Management. We surveyed 220 sysadmins engaged in Patch Management to investigate self-reported behaviors. We found that dedicated testing environments are not as prevalent as previously assumed. We also expand on known behaviours that sysadmins perform when facing a troublesome patch, such as employing a range of problem solving behaviours to inform their patching decisions.

CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; **Vulnerability management**; • **Human-centered computing** → **Empirical studies in HCI**; • **Social and professional topics** → *Software maintenance.*

KEYWORDS

software updates, system administrators, patch management, survey

ACM Reference Format:
Adam Jenkins, Linsen Liu, Maria Wolters, and Kami Vaniea. 2024. Not as easy as just update: Survey of System Administrators and Patching Behaviours. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3613904.3642456

CHI '24, May 11–16, 2024, Honolulu, HI, USA

ACM ISBN 979-8-4007-0330-0/24/05…$15.00
https://doi.org/10.1145/3613904.3642456

1 INTRODUCTION

Patches (a.k.a. software updates) change existing software with the goal of improving it in some way, such as correcting a security vulnerability or adding a new feature. However, software can behave very differently on different systems, setups, and configurations. Updates sometimes change software in undesirable ways that are not necessarily known to the vendor ahead of patch release, such as a Windows update unexpectedly deleting files [1]. Such changes can be incredibly annoying for individuals, but when they happen to an organization they can impact key functions. For example: Google search going offline [11]; Microsoft Office tools going offline [42]; or even Akamai's DNS becoming buggy resulting in many sites effectively going offline [49]. Such problematic patches can cause serious consequences for an organization as well as their direct and indirect customers.

The potential for problems with patches means that automatically installing all patches as they are released is simply too risky for most organizations. Instead they employ System Administrators (sysadmins) who, among other tasks, engage in Patch Management where they monitor for new patches being released, prioritize them, decide if and when to install them, prepare for the update, test for potential problems, and then troubleshoot any resulting issues. The decisions such sysadmins make can have a large impact on the security of their organizations as well as the productivity of the staff they support [31]. A problematic patch can bring down business essential services, causing revenue losses or interruptions to colleagues' working practices [16]. On the other hand, if sysadmins delay or avoid a patch, they leave their systems vulnerable to attack [8, 17] which can similarly negatively impact a business.

Recent work has studied the processes sysadmins go through when engaging in Patch Management [37, 54]. Like other aspects of system administration, Patch Management requires significant coordination among sysadmins [16]. Sysadmins also rely on a wide range of information sources when making their decisions and troubleshooting problems [28, 39]. These works highlight that sysadmins work hard to make good decisions in the face of uncertainty caused by unknown patch impacts. Gaining information is a key part of how they manage issues as well as using resources such as dedicated testing environments and online communities where they can learn from the experiences of peers.

While most sysadmins roughly go through a similar process when patching, contextual factors like the size of their organization

and the types of systems they administer likely have an impact on how they approach Patch Management. A sysadmin working for a large organization likely has access to a test system that mirrors the production servers, giving them the ability to approach patching differently from someone who works for a small organization that only uses Windows clients and has limited testing infrastructure. To test this theory, we conducted a survey of 220 sysadmins who engage in Patch Management related tasks. We combined existing work on sysadmin patch practices to structure the survey and provide answer options likely to match most sysadmins' situations. We then examined how working contexts such as organization size and type of system administered impacted self-reported patching practices. By combining both the behaviours explored by previous survey works [37, 54] and qualitative works [16, 17, 28] we are able to provide a comprehensive view of patching behaviours, confirming and extending upon previous observations and results. The comparatively large survey sample compliments and expands on prior work findings, and our research questions are as follows:

RQ1 Which practices do sysadmins engage in during the different stages of the patching process, and how prevalent are the practices?
RQ2 How does the work context of a sysadmin (e.g. organization size, system type supported) impact patching practices?

Our results indicate that generally sysadmins' approach to Patch Management remains consistent across work contexts. When a patch causes issues, sysadmins will work closely with their colleagues and external communities to problem solve issues. A finding that is consistent with an earlier content analysis of a long-running email list serve dedicated to patch management [28]. Our work shows that their finding holds for the wider patching community and is not isolated to the observed community of practice [64]. Participants in previous research [37, 54] mentioned using dedicated testing environments as a risk management approach. While testing is widely considered best practice, our results show that dedicated test environments are not prevalent and many admins test on a couple of machines or conduct staged deployment instead. We observe that sysadmins turn to online community spaces such as blogs, mailing lists, or subreddits to supplement the information available to them before patching or when trying to troubleshoot issues. We find that these communities remain a source of knowledge in the post-installation stage. Previous work has found that a common response to an error-inducing-patch was to uninstall it from the affected system [37]. Our results indicate that admins will attempt to problem solve any issues by looking to external online sources, like forums, or perform on-site debugging with their colleagues to find a solution, which aligns with their known role of being 'technical brokers' [60] that gather and apply information about the systems they manage.

We recommend that guidance around Patch Management keep in mind that sysadmins have a range of testing resources available to them, and many are unable to conduct dedicated testing before deployment. Future work might consider the value of different types of testing in terms of costs and finding issues, especially when combined with readily available online community information. Future work should also be focused on developing tools which facilitate the debugging and collaboration found within these online sources [28, 29].

2 RELATED WORK

To frame our work we will provide some background on how vulnerabilities and Patch Management relate. We also detail the literature on sysadmins, their working practices, involvement in cybersecurity related tasks, and their roles in the Patch Management process.

2.1 Vulnerabilities and Patch Management

To maintain the security of their systems and users, organizations employ a number of distinct and complementary practices. One such practice is Vulnerability Management (VM), where potential vulnerabilities are actively detected, reduced, or eliminated. Patch Management is theoretically the optimal way to manage vulnerabilities, since a patched vulnerability is removed and can no longer be exploited. Hence it is the approach recommended by groups like the NCSC [44] and NIST [40].

Advice provided by both cybersecurity professionals and government guidance states that the ideal state is for a system to have all software updated to the latest versions [26, 45, 47]. However studies have found that organizations are far from achieving this goal [18, 36, 43, 48]. For example, Setayeshfar et al. [48] examined the patching behaviours of a single enterprise, analyzing 113,675 unique programs used by 774 computers over a 3 year period. They found that the application of updates could range from 10 minutes to several years. Time is critical Patch Management metric, known as "time to patch", since once a vulnerability has been publicly disclosed the volume of attacks using that vulnerability increase by five orders of magnitude. Cyber criminals monitor for new patch announcements and use the information in the patch to design attacks that target the patched vulnerability [9]. In other words, a patch release is effectively a detailed announcement of the existence of a vulnerability, so patching quickly is vital to ensure the patch is in place before criminals can create attacks. Research has shown that the decision to delay patching can result in months or even year-long windows of vulnerability [36, 48].

Automating the deployment of patches is not sufficient due to the *socio-technical* aspects relevant to patching decisions [15, 43, 48, 50]. Previous research [37, 54] and government guidance [40, 45] routinely states that testing patches before installation is best practice. Testing could come in the form of staged deployment, or the use of a dedicated testing environment. The systematic Patch Management literature review by Dissanyake et al. [15] identified 14 socio-technical challenges to software security Patch Management, including the impact of organizational policies, the need for human expertise, and the difficulties in coordination and collaboration around patch deployments. These common challenges delay the application of patches and are detrimental to a system's security as they increase the time to patch and therefore the window of vulnerability.

The race to apply patches before they are actively exploited is countered by the opposing risk of applying updates to system that inadvertently introduce new "bugs" and hence impact business essential operations [8, 15, 50].

2.2 System Administrators and Working Practices

The day-to-day management of IT systems for many organizations and customers is delivered by sysadmins, either organised into distinct teams with a specific service focus (i.e. Network Administration) or by a sole administrator. Sysadmins are considered "*Broker Technicians*" [60] because they gather information and put it in context allowing them to translate between infrastructure users and the developers of the technology in the context of the wider technical community. Information sources are highly valuable to sysadmins in their day-to-day work, as users express requirements, which must be translated into a technical query to the wider community, and then any response and action must again be translated for their organization and stakeholders.

The earliest attempt at understanding the complexities of System Administration at scale was by Hrebec and Striber [25] in 2001, who developed a survey ($N = 54$) to investigate sysadmins' mental models and situational awareness. They found that sysadmins do not fully understand the systems they administer, with an average reported understanding of around 77%. The result speaks to the non-homogeneous and complex nature of modern IT infrastructure. Additionally, when asked how they fix problems they are unfamiliar with, responses included research and investigation of documentation (24%) and experimentation with the system (37%). Sysadmins also reported conducting research online with newsgroups (44%) and consulting personal networks and contacts to find relevant expertise (25%). The results highlighted the wide range of sources and approaches that sysadmins take when managing large complicated systems.

The majority of what is known regarding the working practices of sysadmins is detailed in a series of ethnographic studies [3–7, 22–24, 30, 38] conducted in the early 2000s, and later compiled into a book [31]. The authors detail numerous lessons learned from their observations, including a reliance on developing and adapting best practices or tools to suit sysadmins idiosyncratic working contexts. Sysadmins would continually develop practices with varying lifespans ranging from one-time use to an organization-wide standard. Where they were unable to find a suitable tool or example, they would construct or adapt something suitable. The authors find that system administration is fundamentally a collaborative endeavour as modern IT systems are constructed from numerous distinct systems managed between numerous teams of admins with different but complementary expertise and focus. For example, handling a reported phishing email might involve admins associated with firewalls (block links), email server (remove email), computer accounts (reset compromised accounts), and security (identify threats) [2]. Such collaboration across teams is a common event for sysadmins.

Given the complex and high-risk environment of sysadmins' work, they value tools' accuracy, verification, reliability, and credibility as well as the information they produce [58]. As a result, sysadmin tools require an alternative design approach to those used by end-users [59]. For example the authors highlight the need for tool "flexibility" and "scalability" to suit the working practices of sysadmins who will work with their own unique systems which continually change and represent a diverse range of components. Velasquez and Durckiova [57] discussed the relationship between task complexity and the need for verification information. Essentially, sysadmins are likely to engage in information seeking behaviours when confronted with a complex technical issue, taking in information and translating it to their contexts, and validating that actions performed have had the intended result.

More recently, we have seen the impact of the COVID 19 pandemic on their working practices [32]. Sysadmins' work is inherently collaborative [31] and the work-from-home nature of the pandemic resulted in challenges around coordinating their actions with others.

2.3 Sysadmins and Security

The security of organizations particularly rests on sysadmins given their role of system maintenance and upkeep. For example, sysadmins can influence their system and its users security through configuration errors [14, 65, 66], and with the implementation of SSL [20], HTTPS [35, 55], and firewalls [62].

Security orientated sysadmins and their work practices differ from those in a non-security context. This difference is related to the nature of cybersecurity, requiring a steeper learning curve and a more reactive approach to events that are high risk and complex, resulting in a stronger focus on collaboration [22, 30].

2.3.1 Sysadmins and the Patching Process. Balancing the costs, benefits, and risks of patching has been an ongoing point of research. Shostack detailed the balancing act that is at the heart of patching decisions made by sysadmins, as they weigh out and compare the potential risks associated with installing a patch to a business essential systems against the security risks of not installing and leaving a vulnerability with the system [50]. This work was influenced by the work of Beattie et al. [8], who developed a model to identify the optimal time for an update to be applied. Their model found that the optimal update times in 2002 fell on 10 and 30 days following the initial release of a patch. Upon release patches may contain errors which are then found as people install the patch and corrected through the release of hotfixes. By waiting to install sysadmins can install the corrected version, they can also tap into their personal networks to learn what impacts the patch is having on other systems before making installation decisions.

While developing a distributed framework for deploying patches, called Mirage, Cameri et al. surveyed 50 sysadmins [12] in 2007. Their results showed that patching is a regular occurrence with 90% of respondents handling patches at least once a month. Furthermore, 70% reported delaying the installation of an update and the average failure rate of patches was reported to be 8.6%.

More recently we have seen research that has focused solely on sysadmins and Patch Management, with Li et al. [37] conducting a survey (n=102) and semi-structured interviews to identify the typical actions performed by sysadmins during the patching process. They identified 5 stages of patching, and how the stages impact patching effectiveness. For example, they observed that due to a lack of a single centralised hub of patching information, sysadmins were forced to search a number of different sources to gather information on patches. The survey responses included: official vendor notifications (71%), security advisories (78%), professional mailing lists (54%), online forums (53%), news (39%), and blogs (38%). When asked how they would handle patches which cause errors,

just under half of respondents (47%) reported they would uninstall the update, which may leave their systems open to compromise. This work was extended upon by Tiefenau et al. [54], who showed similar results with a smaller survey (n=67) of a predominantly European sample of sysadmins. They identified a number of additional obstacles including the scheduling of necessary system downtime for patch installation (88%). An interesting observation from their results was that 55% of respondents reported that post-deployment errors from updates were a minor concern, with only 8 participants strongly disagreeing with this statement.

Jenkins et al. [28] analysed the the PatchManagement.org mailing list, which self-describes as the first industry mailing list focused on the discussion of Patch Management and related topics. Using a qualitative analysis of the emails posted, they identified themes such as "Errors and Troubleshooting" where sysadmins would discuss issues faced during that month's patching schedules and negotiate the suitability of potential workarounds available to them. Additionally, "Patch Prioritisation" was identified as a large topic, where email threads would be generated around released patches and discussion of the most security critical updates to install. The authors also identified that the mailing list was an online Community of Practice [64] created from the need for such information given the complexity of patching information and errors.

Martius and Tiefenau [39] focused on release notes of patches and the information sysadmins found useful to inform their patching decisions. To do so they compiled information that was contained within release notes and constructed two surveys (n=41 & n=16) of sysadmins to identify what information was regarded as important. The results showed that 68% of sysadmins found the lack of patch information made the task of patching more difficult, and that *Known Issues* regarding a patch were highly valued. Additionally, the authors noted the lack of standards regarding patch release note contents, resulting in an additional complexity due to managing multiple systems and software components.

Dissanayake et al. [16] used grounded theory to investigate the role of coordination when handling patching decisions. The data was gathered from two organizations over 9 months, with observations of 51 patch orientated meetings. Their work highlights the intricacies within patching, such as the impact of *constraints* which caused disruption in coordination. A good example is *legacy software dependencies* which pose a security risk and create breakdowns in the update process, as these dependent systems need to be updated before any new patches can be applied. Additionally, a *lack of automated support* caused further delays or breakdowns as team members were forced to spend hours manually sorting, searching, and addressing errors or issues raised during the patching process. The second work [17] complements these findings by using a mixed methods approach to identify why and how patches can be delayed during the patching cycle for two organizations within the healthcare sector. Through analysis of 132 delayed patches over 4 years, the authors were able to highlight valuable reasons as to why such delays occur. Among the themes identified they found that *organizational delays* could play a role, such as the impact of policies or schedules which related to the need for certain impacted services being accessible and avoiding system downtime due to reboots.

While the above work has provided valuable insights there are still some important gaps. There is wide agreement that testing patches before installation is an effective approach but we don't know how common the practice is or if admins have access to required test setups. Organization structure also clearly plays a role in decision making, but how often organization policies directly impact patching choices is still unknown. Prior work also shows that admins use a range of information sources, but the work also shows some variation in the type of information used and for what purpose, further information could clarify this point.

2.3.2 The Patching Process. Patching is not a singular event for sysadmins, like many of the activities they engage in, it requires activities like preparation, information gathering, and troubleshooting. The types of information needed, organizational pressures, resource needs, and actions taken all are likely different depending on the part of the patching process the sysadmin is currently in. Prior work has focused on investigating the Patch Management process used by sysadmins and the stages involved [17, 37, 54]. These stages follow a similar pattern to the patching stages end-users use [56] though the scale and complexity are quite different. Below we detail a synthesized version of the stages drawn from prior work. We highlight the sysadmin's purpose and goals within each stage. We use the stages to help structure the survey and select key high level questions to answer. The stages and related high-level questions are listed in Table 1.

1. Awareness. The initial stage of patching begins with becoming *aware* of the need to patch, or that there is a new patch available. This information can be found through a number of channels, including through vulnerability scanning. Previous research has highlighted the wealth of avenues for admins to become aware [28, 37, 39, 54]. This stage is about discovering that a new patch is available, which is an ongoing process due to the continual release of new versions and security related fixes. Even vendors like Microsoft, who famously release patches on a set day each month, release patches and hotfixes off cycle, requiring admins to continually manage their awareness.

2. Prioritisation. Once sysadmins and organizations have identified a need for updates, they must then *prioritise* which updates should be applied and what timeline is needed for their timely application [17]. This prioritization can include factors such as the severity of the vulnerability being addressed, the systems involved, and their integration in the organizations' day-to-day running. Additionally, human factors were highlighted, such as access to integral systems, and factoring in potential downtime resultant from installation.

3. Deciding. Similar to the previous stage, sysadmins must then coordinate within their organization to *decide* when to update. This process can involve sysadmins working closely with affected parties to find an ideal timing to minimise security concerns as well as impacts on business essential services. Other considered factors include the need for human intervention or the need for complex coordination of involved parties [17, 37, 54].

4. Preparation. Systems to be patched may not be fully ready for the installation of updates, hence the technical aspect and patches themselves must be *prepared* in advance. Here, sysadmins may create back-ups of impacted systems or create virtual environments

to uphold run-time goals (i.e. the 'five nines', a systems and its services should be highly available, and that the downtime is less than 5 minutes and 15 seconds per year [1]) for the organization they serve [37, 54].

5. Testing. Most standards and literature emphasises the need to *test* updates before they are applied. This stage can be done through strategies such as testing on personal machines, or formal testing procedures on dedicated testing environments to mitigate the impact of potentially erroneous patches [28, 37, 54]. By testing, and performing staged roll-out of patches, sysadmins are able to gradually apply updates in such a way that a complete loss of systems can be avoided.

6. Installation. Sysadmins will then apply the chosen patches to their systems in some manner. This stage usually takes the form of automation where there exits a large number of systems in which updates are needed [37, 54] or in some instances must be done manually due to the unique nature of the system and can therefore contribute to delays in their application [17].

7. Post-installation. Patches may not be perfect, and can introduce unforeseen issues and technical errors which must then be addressed by sysadmins [29, 37, 54] post-installation. Previous work has indicated that a quick-fix used is to simply remove the update from the systems, resulting in a quick fix but also extending and delaying the remediation of vulnerabilities from the system [37]. However, in doing so workarounds must be sought to mitigate the potential for the vulnerability to be exploited [28, 29].

The process highlighted above is an adaptable flow which in practice may not be as linear as we have detailed. Sysadmin are adaptable and can jump to and from different stages due to information revealed in complimentary stages. For example, sysadmins may prioritize (e.g., stage 2) certain patches due to severity ratings, but they may have to seek workarounds (e.g., stage 6) due to interruptions arising from the need to keep the intended system running for business commitments (e.g., stage 3) or due to issues highlighted during testing of patch quality (e.g., stage 5) [17, 29].

3 METHODOLOGY

We decided to use a survey methodological approach to collect information from a wide range of geographically dispersed sysadmins. The survey was designed based on prior work, particularly qualitative work that explored sysadmins' work practices [28, 37, 54], and the patch management process stages outlined in Section 2.3.2. Consequently, the survey is designed to extend, confirm, and expand on the findings of these works.

Below we describe the survey design, sample, and statistical analysis used. Ethical approval was granted by the Research Ethics Committee of the School of Informatics, at the University of Edinburgh. All design decisions were made in-line with Edinburgh's guidance on ethical survey design.

3.1 Survey Development

Previous research found that sysadmins and other IT Security professionals have hectic working practices making them hard to source for more involved studies [27, 34]. Therefore, our focus was to construct a survey that would take participants no longer than 10 minutes to complete.

Admins can be responsible for a wide range of systems which may have different management strategies. To ground their answers, they were asked to select a specific type of system (i.e. Client, Server, Router, etc.) and answer the questions about that system. We believed that doing so would reduce the complexity when recalling the frequency of their patching actions without needing to estimate across the wide range of technologies they are likely tasked with managing [31].

The first version of the survey was designed by the first and second authors to ensure coverage of relevant behaviours and actions. The questions were then refined in collaboration with the remaining authors. The survey was piloted with HCI and Usable Security researchers ($N = 8$) within our research lab, including respondents whose first language was not English. Additionally, we provided an early version of this survey to four people who were involved in the practice of System Administration, Patch Management, or were moderators of sysadmin related forums or subreddits ($N = 4$). These pilots were done to clarify wording and ensure that the survey questions and options covered what practitioners would expect to see. All comments and feedback were incorporated. The final survey text is in the supplementary materials as well as the TULiPS website[2].

3.2 Survey Instrument

3.2.1 Organization, Working Context, and Baseline. After asking for consent, we asked how many distinct organizations sysadmins manage patches for, to account for those who work for outsourcing companies. For those who work for more than one organization, we asked them to select only one when answering the remaining questions.

We then asked for details about the organization (sector, number of employees in organization, number of other sysadmins they worked with). Then the technical environment that they managed. Including the type of machines (servers, clients, mobile, routers/network, IoT, other), number of machines, and type of Operating Systems (OSs) managed. Additionally, we asked for the types of software of components they were in charge of patching (OS, applications, custom/bespoke, no longer supported by vendor). No longer supported software was specifically included in the list as it is known to be more challenging to manage [17].

Finally, we asked respondents to select one of the types of systems they supported, and to answer all following questions based on that system and its OS, henceforth refereed to as the "baseline set-up". This was done to allow us to compare between groups based on systems and to investigate any potential differences in their behaviours.

3.2.2 Patching Behaviours and Actions. This section of questions was modeled after the stages of the Patch Management process described in Section 2.3.2. Question wording and options were were based on the the findings of previous research [15–17, 28, 37, 39, 54]. The first author and second author individually read each of the

[1] https://en.wikipedia.org/wiki/High_availability#Percentage_calculation

[2] Survey Text: https://tulipslab.org/projects/patch-management/CHI2024-admin-survey.pdf

Patching Stage	Question
Awareness	When new patches become available, I learn about them through:
Prioritisation	When deciding which patches to prioritise for installation or testing, how often do you engage in each of the following?
Deciding	Who makes the final decision about installing, not installing, or waiting to install a patch? In your opinion, how much say do you have in if a patch will or will not be installed?
Preparation	When preparing to install patches on a system, how often would you do the the following actions?
Testing	When testing patches which of the following test setups do you use? What most motivated your testing setup When testing patches, what is considered by your organization? (Only shown if they test patches.)
Installation	The deployment of patches is:
Post-Installation	Once a patch has been deployed, to validate that it is working as expected, I will: When you detect an error after testing or deployment, what actions would you perform?

Table 1: List of patching stages and the related survey questions. Each of the above questions was close-ended, using three formats: multiple choice (radiobox), multiple answer (checkbox), or a set of Likert options. When appropriate, an "other" option was also provided that allowed for free text entry.

previous related works, gathering stated behaviours in the articles and the related methods (i.e. survey instruments and interview scripts). Once each work had been independently covered by the authors, we met to aggregate behaviours into the form of questions grouped by the respective patching stages. The main question text along with the patching stage it corresponds to can be seen in Table 1. Questions for Awareness, Prioritisation, and Preparation, were block questions with the rows being common answers from prior research and the columns being Likert frequency options from 'Never' to 'Always'. Questions for Deciding, Testing, and Post-installation were singular questions with answer options that were drawn from prior work [16, 17, 28, 37, 39, 54]. Questions, the behaviours they captured, and their wording were then checked through Think-Aloud interviews with 2 experts with sysadmins experience. Finally, questions were checked by moderators of our chosen subreddits (detailed below) and the PatchManagement.org mailing list.

We placed a simple attention check question that asked respondents to select the option "Sometimes" in the Preparation question block. Respondents who failed this attention check were removed for analysis.

3.2.3 Demographics and Anything Else. Demographics included information about the respondents' highest education, gender, experience with system administration, job title, years in role, and country they work in. Finally, we ended with an optional open ended question, which allowed respondents to provide any other information regarding the patching process that was not captured within our survey.

3.3 Participant Recruitment

The survey was implemented using Qualtrics and distributed using an anonymous link. To collect the widest sample of professional sysadmins possible we took a snowball sampling approach and recruited through a number of channels known to have previously been successful in recruiting sysadmins [37, 39, 54]. These included relevant subreddits on the social media platform Reddit [3], such as r/sysadmin, r/windows, r/linuxadmin, r/windows10, and r/windows11. We actively sought approval from moderators from all utilised subreddits before posting our survey to avoid breaking any community norms. Additionally, we shared our survey with the moderators of PatchManagement.org [4], who circulated the survey through the mailing list. Moderators for both the mailing list and the chosen subreddits explicitly asked that the survey instrument used did not use any from of tracking due to the rules of the respective communities, and the concerns raised regarding responses being heavily linked with job security and performance. Hence plain links were used that did not track recruitment source and IP addresses were not collected.

We also posted our survey to Twitter and encouraged known security professionals to share the survey to additional relevant groups or channels.

The survey was active for 2 full weeks, from August 24 to September 7, 2021. These dates were selected to avoid weeks surrounding and including Microsoft's Patch Tuesday, as sysadmins are known to be very busy during that time [28]. We did not provide participants with payment or the opportunity of prizes and instead highlighted our interest in improving the state of patching and that any published works would be shared with the participating communities.

During the time that the survey was live, 362 respondents started the survey, and 224 (61.5%) completed all essential questions. We removed 4 responses who failed our attention check question, resulting in a final sample of 220. We manually checked the accuracy and validity of the remaining results of the responses which scored higher than the recommended value of 30 for the Qualtrics value 'Q_RelevantIDFraudScore [5]. This check resulted in 5 responses which were checked for consistency of responses and additional checks were made with the responses submitted in the open-ended questions. Following these checks, we were satisfied that all 5 responses were legitimate to the best of our knowledge and were retained in the final set of 220 responses. The median time for the survey was found to be 8 minutes and 13 seconds (min=3 minutes 38 seconds, max= 176 minutes 43 seconds). The two responses that were found to be outliers (4 hours 22 minutes, and 7 hours 44 minutes) were manually checked. Since their answers seemed logical

[3]https://www.reddit.com

[4]https://www.patchmanagement.org

[5]https://www.qualtrics.com/support/survey-platform/survey-module/survey-checker/fraud-detection/#RelevantID (N=5)

and in line with our dataset, they were kept. We believe these times are participants returning to finish their responses or artefacts of the timing mechanism within Qualtrics itself.

3.4 Statistical Analysis

Comparisons between groups were made using scipy.stats package, version 1.3.1 [61]. We used non-parametric Mann-Whitney tests to compare questions using Likert scores such as for sysadmins' reports of frequency of behaviours in the Awareness, Prioritisation, and Preparation stages of the patching process, as seen in Table 1. For Likert-based questions, which consisted of 7-9 statements, we used Bonferroni Correction to adjust for multiple comparisons. We only report results which are statistically significant at the $p < 0.005$ level (significance threshold: 0.005 = 0.05 / 10, where 10 is the upper limit of the number of comparisons within one set of Likert statements). To compare groups for questions which allowed participants to select a single option, we used Chi-square tests.

4 RESULTS

In this section we detail the respondents' demographics and their working contexts, such as the organizations they work for, and the technical make-up of the environments that they manage. Following this we detail the responses for actions and behaviours associated with the patching process, and include some statistical comparisons based on splitting our sample by organisation size and type of machine managed.

4.1 Participants

A summary of the participants' demographics can be found in Table 2. The vast majority of our responses came from males (86%, N=190), with only 13 (6%) identifying as female, 2 non-binary, and 1 choosing to self identify. The most common age band reported was 25-35 (32%, N=71), followed closely by the age bands 35-45 (28%, N=61) and 45-55 (18%, N=40). The majority of participants had received some form of higher education with a total of 173 (79%) reporting at least attending college, with a Bachelor's degree being the most common qualification attained (39%, N=86). The majority of our sample was from North America (57%, N=126), with the two largest groups following this being Europe (20%, N=43) and the UK including Northern Ireland (15%, N=34). Respondents were generally experienced system administrators with over half having 11+ years of experience (51%, N=112), 46 (21%) with 6-10 years, 36 (16%) with 3-5 years, and 17 (8%) with 2 years or less.

4.1.1 Organizations. Table 3 summarizes the organizations respondents work for. The overwhelming majority manage patches for a single organization (76%, N=168), however 50 respondents (23%) reported patching for more organizations, these are likely employed at an IT outsourcing company. 2 respondents were unemployed at the time of the survey. Just under two thirds of respondents' organizations had over 250 employees (N=138; 63%), and 46 (21%) reported organizations of 50 to 249 employees. The most common sectors were technology (N=36, 16%), education (N=31, 14%), government (N=28, 13%), and healthcare (N=20, 9%).

4.1.2 Managed Machines and Software. Table 4 summarizes the work environments of respondents. The majority reported working

		N	%(2d.p.)
Age	18-25	20	9.09
	25-35	71	32.27
	35-45	61	27.73
	45-55	40	18.18
	55-65	11	5.00
	Over 65	4	1.82
	Prefer not to say	13	5.91
Gender	Male	190	86.36
	Female	13	5.91
	Non-Binary/ Third Gender	2	0.91
	Self Identifying	1	0.45
	Prefer not to say	14	6.36
Location of Work	North America	126	57.27
	UK and Northern Ireland	34	115.45
	Europe	43	19.54
	Asia	2	0.91
	Oceania	8	3.64
	Caribbean	1	0.45
	Prefer not to say	6	2.73
Education	Secondary School or Less	1	0.45
	High School	24	10.91
	College but no degree	55	25.00
	Bachelor's	86	39.09
	Master's	29	13.18
	PhD	3	1.36
	Other	15	6.82
	Prefer not to say	7	3.18
Sysadmin Experience	< 1 year	3	1.36
	1-2 years	14	6.36
	3-5 years	36	16.36
	6-10 years	46	20.91
	11+ years	112	50.91
	Prefer not to say	9	4.09

Table 2: Participant Demographics: Age, gender, location of work, education level, and experience with System Administration (N=220).

with colleagues, with only 31 respondents reporting working alone. Just over a third of respondents reported managing over a thousand machines (N=82, 37%). Sysadmins in our survey managed a range of software types, with only 39 (18%) respondents reporting management of only one type of machine and the majority of these – 31 out of 39 (80%) – managed servers. Servers were the most popular managed system (N=207, 94%) overall, with client machines being the next largest group (N=173, 79%). When asked to provide details regarding the types of software that they managed on their systems, almost all admins reported OS (N=216, 98%), with applications also receiving a large proportion of respondents (N=197, 94%). Interestingly, just over a quarter of respondents reported being in charge of managing software that is no longer supported by the vendor. The most common OS managed was Windows (N=200, 91%), with the next being Linux with 138 respondents (63%).

4.2 Patching Behaviours and the Effect of Organisation and Machine Type

In the following sections, we report claimed patching behaviours, grouped by patch management process stage (c.f. Table 1—RQ1). To examine the effect of work context (RQ2), we compared the frequency of reported behaviour in regards to organisation sizes

		N	%(2d.p.)
No. of Organizations	Single Organization	168	76.36
	2-5 Organizations	21	9.55
	6-10 Organizations	8	3.64
	11+ Organizations	21	9.55
	Unemployed	2	0.91
Organization's Sector	Business & Professional Services	17	7.73
	Communication & Media	7	3.18
	Consumer Staples	15	6.82
	Education	31	14.09
	Energy	4	1.82
	Financial	17	7.73
	Government	28	12.73
	Healthcare	20	9.09
	Manufacturing & Engineering	17	5.91
	Other	18	8.18
	Technology	36	16.36
	Transportation	6	2.73
	Prefer not to say	4	1.82
Organization Size	<10 employees	13	5.91
	10-49 employees	23	10.45
	50-249 employees	46	20.91
	≥ 250 employees	138	62.73

Table 3: Organization Demographics: Respondents' organizations, including size, sector, and number of organizations the respondents manage patches for, N=220.

		N	%
No. Sysadmins work with	0	31	14.09
	1-5	120	54.55
	6-10	26	11.82
	>10	43	19.55
No. of Machines	1-100	38	17.27
	101-250	32	14.55
	251-500	41	18.64
	501-1000	27	12.27
	1000+	82	37.27
Machine Type	Client Machines (Laptops, Desktops etc.)	173	78.64
	Servers	207	94.09
	Mobile Devices (Phones & Tablets)	82	37.27
	Routers/Network Appliances	133	60.45
	Embedded devices/Internet of Things	54	24.55
	Other	12	5.45
Software Managed	Operating System	216	98.18
	Applications	197	89.55
	Custom/Bespoke inhouse programs	79	35.91
	Software that is no longer supported by Vendor	61	27.73
	Other	7	3.18
Operating System Managed	Mac	57	25.91
	Windows	200	90.91
	Linux	138	62.73
	iOS	63	28.64
	Android	55	25.00
	ChromeOS	7	3.18
	Other	26	11.81

Table 4: Work Contexts: Working environments of respondents, detailing the range and types of machines managed, the types of software managed, and the OS types managed. N=220

(large organizations with over 250 employees henceforth refereed to as **LO**, N=138, 63%, versus SMEs with 250 or fewer employees henceforth refereed to as **SME**, N=82, 37%) and machine type. 50% of all respondents (N=109) chose to answer the survey in terms of their work with client machines, while 47% (N=104) chose servers. There were only 6 (3%) respondents who chose to recall their patching process for other machine types, with the majority of those choosing routers and network devices (N=5). From here forward we only focus on responses for clients and servers, and we refer to each group as **CA** and **SA** respectively.

4.2.1 Awareness. We asked our respondents to report the frequency of different potential sources of patch awareness using a Likert scale (Figure 1). The most frequent response was that respondents expected the patch because it was released regularly, with just under three quarters stating most of the time or always (74.9%; N=164). The least common way to become aware of a patch was by being notified by the software itself with just over one eighth of respondents indicating that this occurred most of the time or always (12.8%; N=28).

Microsoft, one of the largest software vendors, regularly releases patches on the second Tuesday of the month (Patch Tuesday). Other vendors follow similar patterns, releasing patches on a regular monthly schedule. This regularity is intended to make it easier for admins to predict when they will need to spend time patching. The result that most admins expect patches to be released on a regular schedule is therefore somewhat expected.

Organization. Sysadmins from the SME are more likely to become aware of patches through notifications from the software itself than sysadmins from the LO group (Mann-Whitney U(137,82)=4259, $p<0.005$). Instead, LO sysadmins were more likely to become aware of patches that were released during regular patching schedules (Mann-Whitney U(137, 82)=4410.5, $p<0.005$). This suggests that large organisation may have specific patching policies around key patch release dates, while sysadmins for SMEs are more sensitive to irregular patches such as hotfixes.

Machine Type. We found no significant differences between CA and SA groups when it came to awareness of patches. This may indicate that their is an established practices and information sources for these two device groups when it relates to how admins gain information about released patches. These practices appear to be managed and acted upon by the chosen online communities of sysadmins, with complimentary but idiosyncratic roles during collaborative acts by online communities [29].

4.2.2 Prioritization. The prioritization question asked how often admins used a range of sources to prioritise patches. Findings are displayed in Figure 2. 68.0% of all respondents (N=149) stated that they never or sometimes perform formal risk assessments for patches. Calculating potential downtime of systems was also less of a concern, with around two thirds stating that they never did it, or sometimes (65.8%; N=144). Patching policies were used as a guide prioritization most of the time or always by about half of respondents (54.3% N=119) which is both one of the most commonly used prioritisation methods, and lower than one might expect given that patching is a key component of many security guidelines. When it comes to integrating external information, 59.4% (N=130) respondents never or sometimes prioritised based on guidance from online sources like forums.

Organization. Patching policy is more likely to play a role in patch decisions in the LO group than in the SME group (LO median = 4 (often), SME median = 3 (about half the time); Mann-Whitney U(137,82)=4300 $p<0.005$). Sysadmins within the SME group are somewhat more likely than those in the LO group to factor in

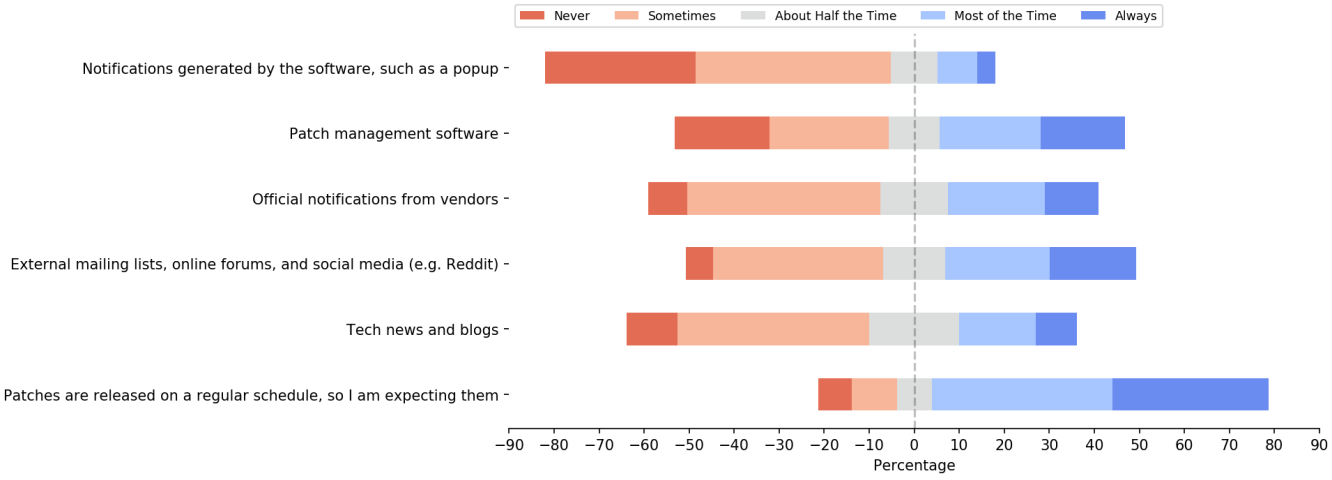

Figure 1: Awareness. Answers to the question: "When new patches become available, I learn about them through:". Results shown as percentages, N=219.

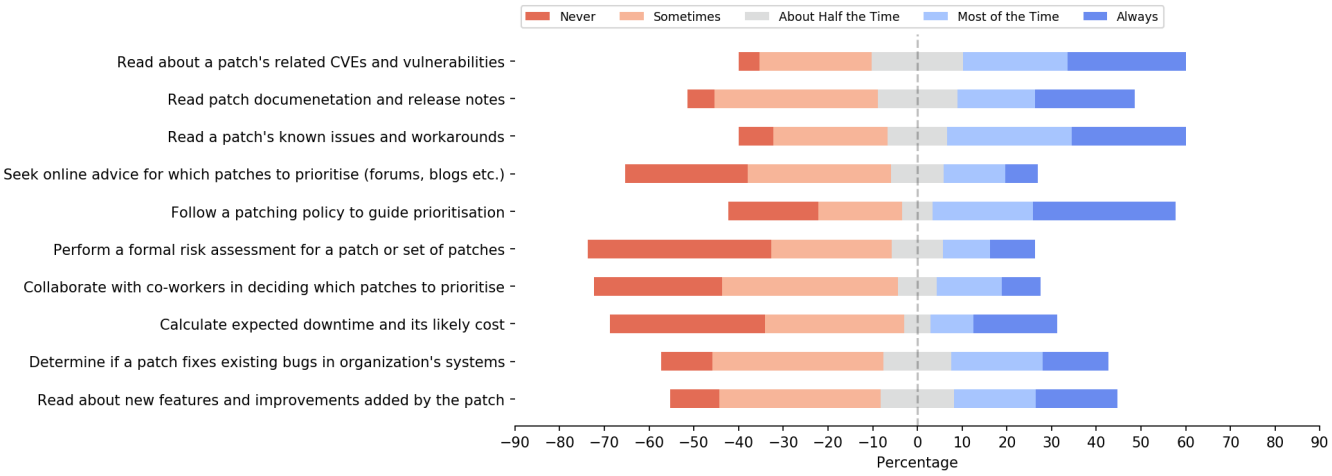

Figure 2: Prioritization. Answers to: "When deciding which patches to prioritise for installation or testing, how often do you engage in each of the following." Answers presented in percentages, N=219.

downtime of affected systems (LO median = 2, SME median = 2; Mann-Whitney U(137,82)=4463.5 $p<0.005$), but in both cases, they are relatively unlikely to do so (median answer for both 2, corresponding to sometimes). This is possibly due to the available when we compare these two groups, as large and established business may have more structured security policies, and additionally will be able to provide additional resources which can dissipate and manage the downtime on business essential systems such that impact is minimally felt.

Machine Type. There were two main differences between sysadmins from the SA group and CA group, with 71.2% of SA (N=74) reporting that they did not rely on external sources to identify and aid in prioritisation, as opposed to 47.7% of CA (N=52). Admins in the CA group were also more amenable to seeking online advice regarding which patches to prioritise (CA median = 3 (half and half), SA median = 2 (sometimes); Mann-Whitney U(109,104)=3927.5 $p<0.005$). This result may be due to the popularity of the Windows OS, making patching related information more accessible with user reports on social media [28] or through the vendor's help forums directly [41]. Furthermore, factors in decisions related to server patches appear to be based on the organizational setting rather than the decisions made for client machines which may be more standardised across different organizations, hence general server advice is potentially being less applicable to themselves and their unique servers.

4.2.3 Deciding. We asked who or what made the decision to patch, not patch, or delay a patch (multi-answer). The overwhelming

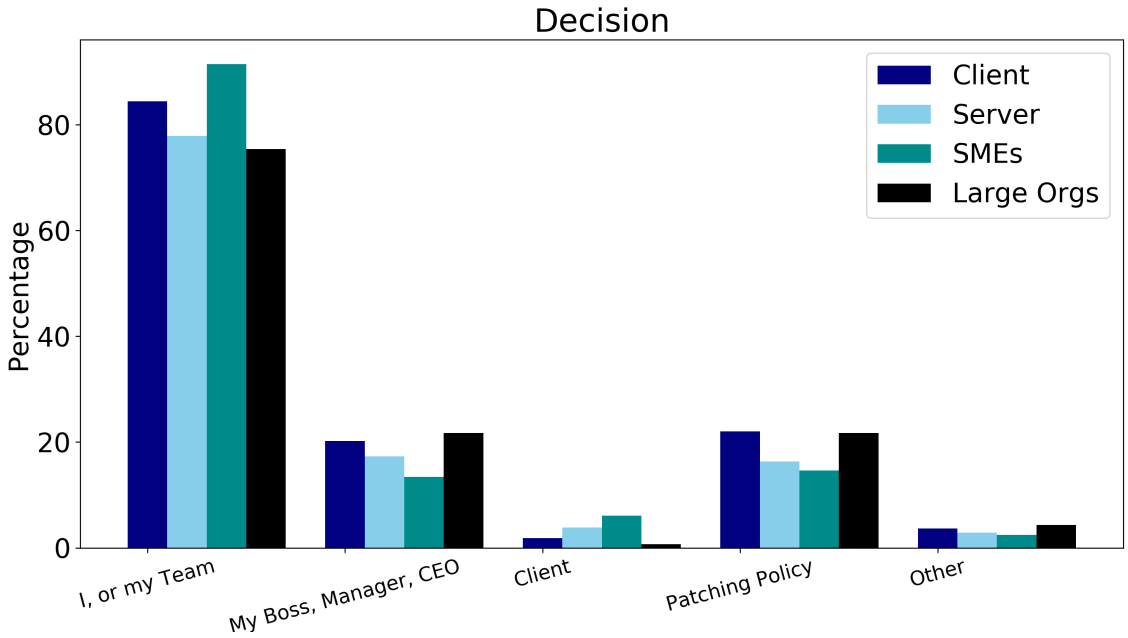

Figure 3: Deciding. Answers to: "Who makes the final decision about installing, not installing, or waiting to install a patch?" Answers broken down by the type of machine being managed and the organization size. Results shown as percentages, N=220.

response from all admins was that it was themselves or their team who made the final patching decision (81.4%; N=179). Only 19% of admins reported that a formal patching policy played a role in their decision process. Additionally, only 18% reported having input from their boss, manager, Chief Information Security Officer (CISO), or another executive from their organization. This result was further compounded when asking respondents to gauge the amount of say they have in the decisions regarding a patch, with over two thirds of admins stating that they had a 'great deal' of input (N=151, 69%) and only 19 respondents (9%) stating they had little to no say in their organizations' patching decisions. All responses are displayed in Figure 3.

Organization. 91.5% of the SME group (N=75) state that they or their team had responsibility for patching decisions as opposed to 75.4% of sysadmins within the LO group (N=104; c.f. Figure 3). Decisions from the LO group appeared more centralised and driven by policy: 21.7% (N=30) of sysadmins in LO reported an influence of their managers, compared to the SME group with 13.4% (N=11). Furthermore, 21.7% (N=30) of LO respondents indicated that patching policy impacted decisions, compared to SME's 14.6% (N=12). Some SME sysadmins reported customer influence on patching decisions (6.1%; N=5), while this was almost never the case in LO (0.7%; N=1).

Machine Type. There was little difference in perceived input in patching decisions scores between that of CS sysadmins and SA sysadmins. Both client and server sysadmins reported that they or their team had the main say in patching decisions.

4.2.4 Preparation. Scheduling a suitable time to patch in collaboration with impacted users was a regular occurrence with 71.8% of all respondents reporting that they did this most of the time or always (N=158). Interestingly, many of the other actions which involved changing or modifying components were considered rare events, with the majority of respondents selecting 'Never' or 'Sometimes'. This included the modification of deployment scripts (81.4%; N=179), configuration files (86.4%; N=190), or settings for third party patching tools (80.9%; N=178). Surprisingly, the action which appeared to split the respondents was the frequency of making back-ups of their systems, with just over half indicating this was a regular occurrence (55.0%; N=121), as seen in Figure 4.

Organization. There appeared to be little differences between the frequency of reported actions by organization size and we found no significant differences.

Machine Type. Backing up the system before patching differed between CA and SA sysadmins. A larger proportion of CA group reported this to be a rare occurrence (50.5%; N=55), compared to SA sysadmins who stated this was regular occurrence (66.3%; N=69). This difference was statistically significant (Mann-Whitney $U(109,104)= 4059.5, p < 0.005$). This result may be due to the fact that sysadmins working with servers may have greater access to backup infrastructure and machines than sysadmins updating client machines. Client machines may include work laptops taken between work and home, limiting direct access and leaving management and the application of patches up to the individual user [32].

4.2.5 Testing. We asked sysadmins to indicate all the patch test setups they use. Overall, we found that only 12% (N=26) reported that no testing was used. Around half reported using staged deployment

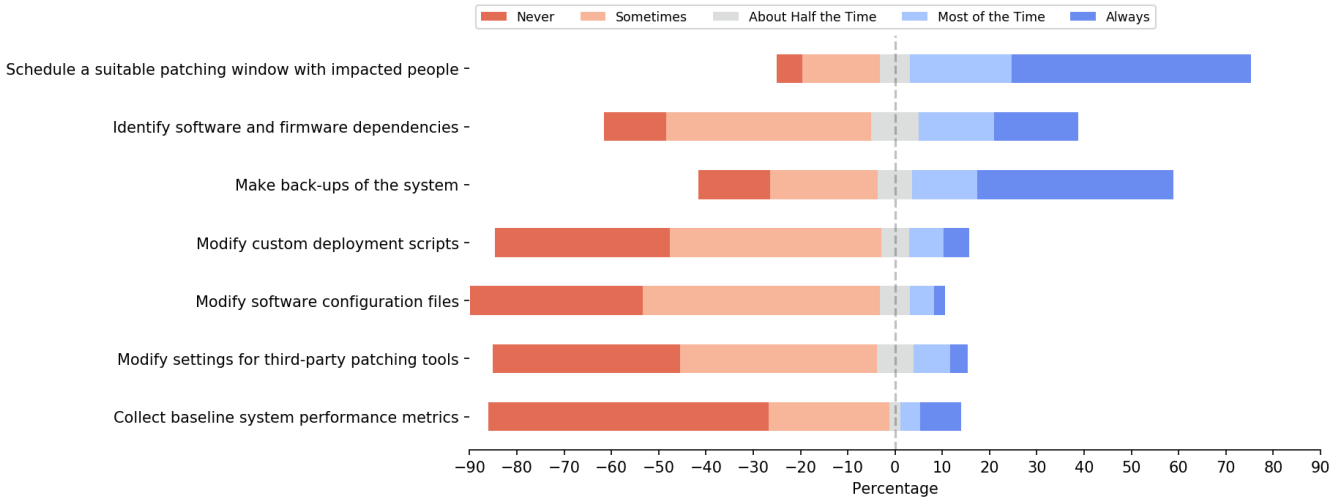

Figure 4: Preparation. Answers to the question: "When preparing to install patches on a system, how often would you do the following actions?" Answers presented as percentages, N=220.

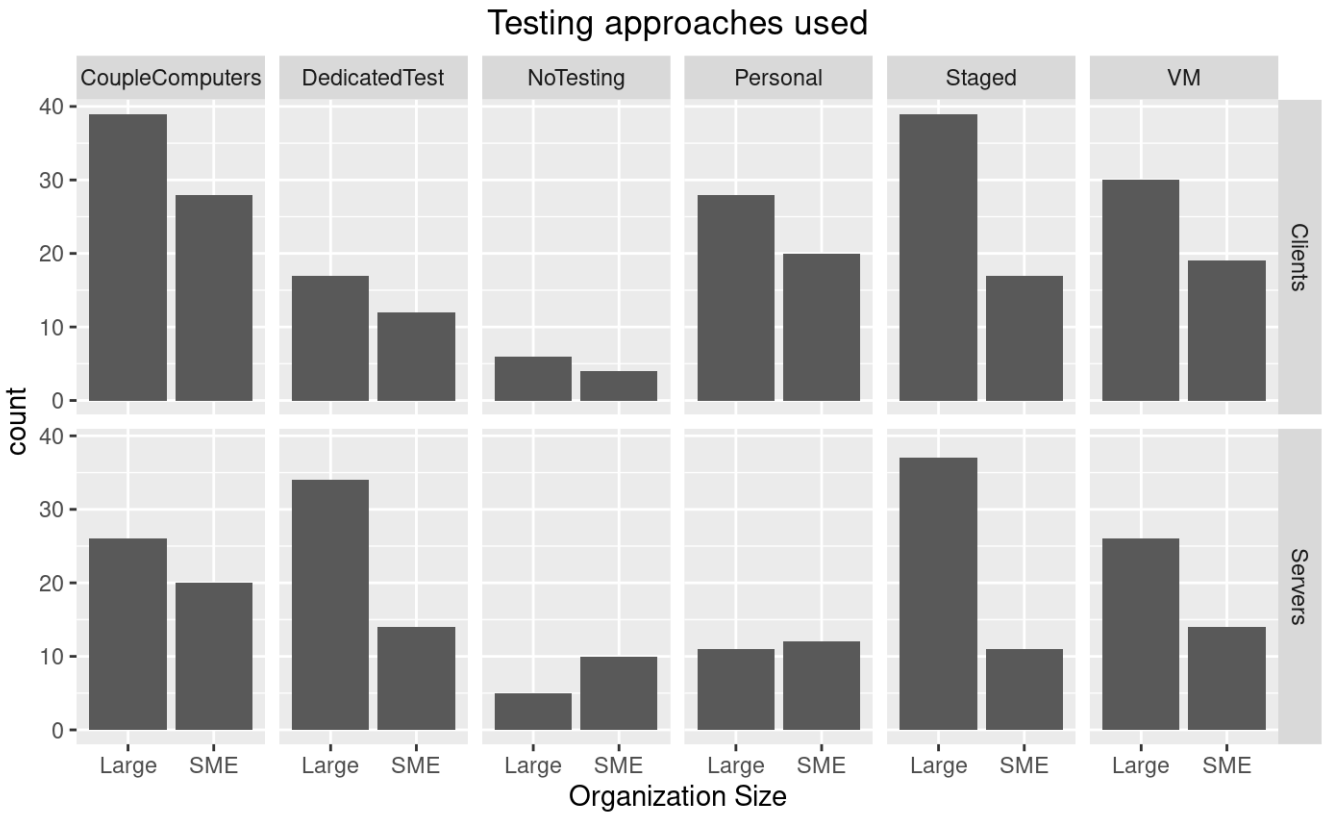

Figure 5: Testing setups used broken down by size of the organization (Large or SME) and the type of system being managed (clients or servers). Multiple answers allowed. Answers of "Other" excluded from graph for readability.

(N=107) as part of their testing process. Dedicated test environments were not as prominent as previously thought [37], with just over a third of admins reporting access to one (36.4%; N=80) as part of their testing process. When asked what motivated their testing set-up, the answers were quite split. "Resource availability" was the most popular option with 25.9% of all admins (N=57); 21.8% (N=48) stated that their patching policies motivated the set-up; and 23.6% (N=52) reported that they were motivated by patches rarely causing errors.

Organizations. When we compare the test setups used by organization size (c.f. Figure 5), a greater proportion of admins from LO (57.2%; N=79) report using staged deployment when compared to SME group (34%; N=28). Another clear difference can be seen in motivations for testing set up, with a greater percentage of admins from LO stating that patching policies motivated their setup (27.5%; N=38) compared to the SME admins(12.2%; N=10). Moreover, 30% (N=25) of SME admins reported that patches rarely caused errors as a motivator compared to large organizations with only 18% (N=25). Organization size was found to influence the reasons selected by admins to justify their chosen testing set up, with a significant difference between selections made by admins from SME and those from the LO group ($\chi^2(4, N=213) = 10.4, p < 0.05$).

Machine Type. There is a clear difference between CA and SA sysadmins' use of dedicated test environments. Only around 27% (N=29) of CA report using test environments, compared to almost half of SA (46.2%; N=48). 14% of SA sysadmins (N=15) reported no testing compared to the CA group (9.2%; N=10). There is no difference by machine type in the reasons cited for using a particular set up ($\chi^2(4, N=207) = 2.2, p > 0.5$). This result suggests that the testing set-up is influenced more by organization size than by type of machine administered. Since small and large organizations likely have differences in budget, resources, and formality of processes available to sysadmins, this result makes sense.

4.2.6 Installation. We asked participants to estimate the level of automation they use in the deployment of patches using a Likert scale. 60% (N=129) of respondents stated that their deployment was "Mostly Automated". The least popular option was "Fully Manual" (5%; N=10). This results makes sense given the growing trend of automation. Prior work has highlighted that patch installation still needs input from a human expert to make decisions [15, 17, 31]. This observation is likely why "Fully Automated" was a more common approach than being "Fully Manual", but still less than both hybrid approaches (15.7%; N=34).

Organizations. "Mostly Automated" patch management is reported by 67% (N=91) of respondents from the LO group and 47% (N=38) of respondents from the SME group. SME sysadmins are more likely to resort to automated and manual patch management equally often (SME: 20% (N=16), large organization 4% (N=6)). This difference in behaviour was statistically significant (Mann-Whitney $U(135,81) = 4280.5, p < 0.05$))

Machine Type. There was no statistical differences found between the admins of CA group and SA group.

4.2.7 Post-Installation. Since one risk of patch installation is the introduction of errors or problems into the system, we also asked about how admins monitor for issues and how they respond if an issue is identified. The most popular response in regards to validating that a patch is working was to monitor user reports (80%, N=174), closely followed by monitoring online sources for reported issues (66.4%, N=146). Respondents were notably less reliant on vendor actions such as announcements (44%; N=96), or changes in patch documentation (24%; N= 52). This result matches prior work observations that admins remain vigilant to online sources to detect potential patch problems [28] and do not solely rely on official and internal channels.

Our final question asked about reactions once an error with a patch has been identified. The most popular strategy was to investigate the cause and scope of the error with 77% (N=169). Checking patch documentation (67.3%; N=148) and reading or asking for help from online sources (66.8%; N=147) were also widespread. Interestingly, only 22.3% (N=49) of all responses reported immediately uninstalling the offending patch. Findings are summarised in Figure 6.

Organization. Sysadmins for SME and LO groups monitor patch performance in very similar ways. However, they differ in their troubleshooting strategies. Raising a ticket with the vendor was reported by only 23.2% (N=19) of SME sysadmins compared to 52.2% (N=72) of sysadmins with the LO group. Additionally, SME sysadmins more often used online forums for help and advice (73.2%; N=60) compared to sysadmins from LO (63%; N=87).

Machine Type. Differences between machine type are similar to those we saw between types of organizations. Fewer sysadmins of the CA group raised tickets with the vendor (33%; N=36) compared to server sysadmins (49%, N=51). CA sysadmins also used online sources to monitor for issues (75%, N=82; SA: 59.7%, N=62), and seek advice (CA: 73.4%, N=80; SA: 63.5%, N=66) more often.

5 DISCUSSION

Prior work has used a mix of qualitative and survey work to understand the workflows and behaviors of system administrators. Their survey work was naturally focused by the outcomes of the qualitative work they based it on. The work presented here expands on these earlier findings by taking into account key issues that were identified by the range of work now available, such as the important role of information sources, and then bringing them together into one survey. Our survey is also designed to look at key issues that occur at the different stages of the patching process such as the role of organization policy when deciding to patch. The availability of earlier works allowed us to build a more comprehensive survey and understanding of how sysadmins from different organization sizes and supported systems approach patching. Our survey provides a stronger case for generalizing earlier findings [16, 17], and offers new insights and avenues for future research within both System Administration, and Patch Management research. In essence, our work highlights the importance that such communities may play in security decisions around patching and navigating issues [28], which is compatible with the literature on this unique user-group and their working practices [31].

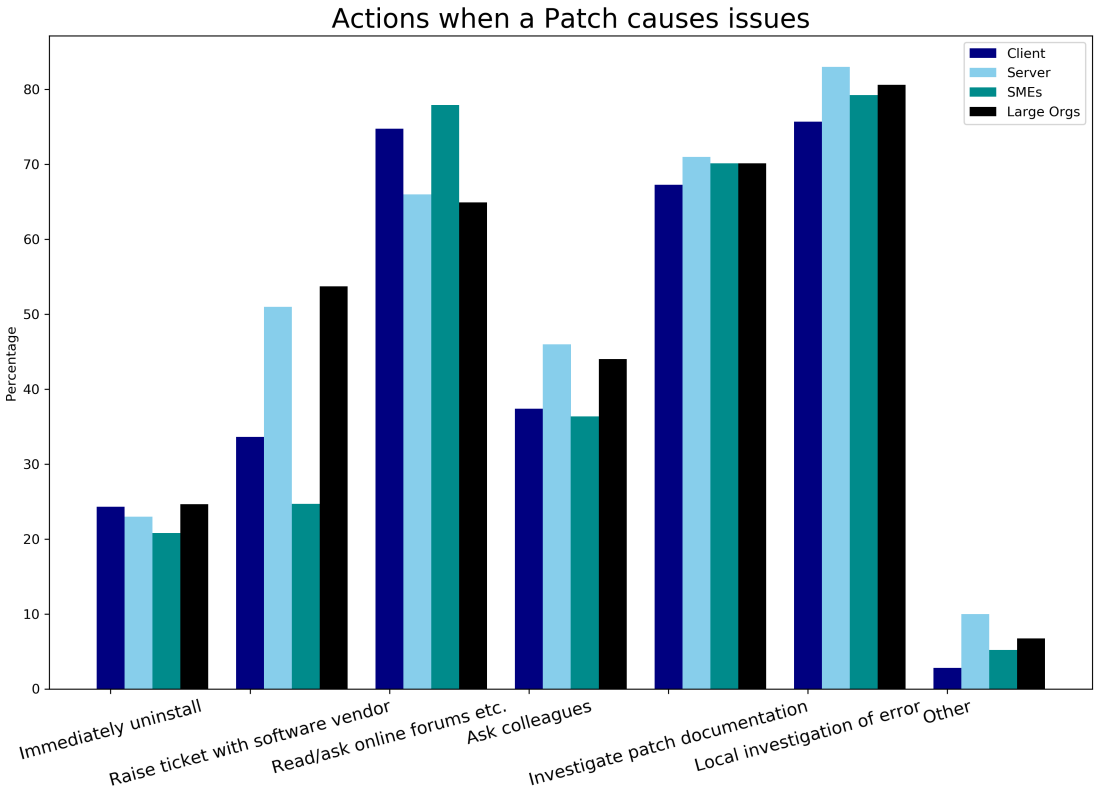

Figure 6: Post-Installation Errors: "When you detect an error after testing or deployment, what actions would you perform?". Answers broken down by the type of machine being managed and the organization size. Multiple responses to this question was possible and results shown as percentages, N=220.

Our results highlight a number of interesting findings, including the contexts in which administers work. Sysadmins are responsible for the patching of a range of systems, and the applications that run on those systems. We found that a quarter of sysadmin surveyed manage software that is no longer supported, adding further complexity to Patch Management. Our results highlight the prevalence of previously identified behaviours [37, 54] and observed behaviours [16, 17, 28] (RQ1), such as the testing set-ups used by admins, with dedicated testing environments and the use of staged deployment less common than previously theorised. We also find minimal difference across work contexts in regards to approaches taken in the patching process, and in the level of input these admins feel they have in patching decision making. We found that admins of servers are less likely to engage with online advice (RQ2). It may be that the server setups are more likely to be specific to organizations making online advice less useful than for client systems which may be more likely to be running popular software and therefore experiences and solutions of others are more likely to be applicable.

5.1 Online information gathering supports most stages of the patching process

Previous work indicated that admins struggle to coordinate their patching process due to the wide ranging number of sources of information, from internal systems, notifications, mailing lists, and news or tech blogs [13, 17, 28, 37, 54]. We found that the process of patching is an ongoing search for information. For example, we showed that sysadmins will monitor online sources for hints and suggestions of errors within patches. Doing so will give admins some forewarning of potential risks associated with a patch, which can be useful in tasks ranging from prioritization, testing, and troubleshooting. Testing setups are also often incomplete and do not capture all the configurations of individual systems, making it challenging to find all potential problems in advance. A simple example is having two 4K monitors, something end-users have but the test setup might not so a patch that disables a monitor might pass basic testing [29]. Keeping on top of these potential issues ensures that sysadmins are prepared when an error suddenly appears.

For patch awareness sysadmins reported not relying on patch management software, which is somewhat counter intuitive as

tracking new patches is one of the primary purposes of such software. This observation may be due to the regular nature of patches, specially within the Microsoft platform, which routinely release all patches on the second Tuesday of every month. This release cycle is known as 'Patch Tuesday' [6]. Additionally, it appears that sysadmins have adapted to the spread of information by forming their own online communities [28, 31] which through their collaborative information gathering efforts have essentially created a proxy centralised source for their patching information needs. Thus, sysadmins have created their own socio-technical resources to alleviate problems. Future research should investigate these online communities, as such cooperative behaviours have previously been highlighted in both patching [16, 28] and in general System Administration [31]. By investigating these communities, we can better understand how they are viewed and used in sysadmins' practice. Such work can also support the development of tools which promote collaboration and allow admins to seek the information relevant to their particular context. For example, we may want to support discussion regarding patch prioritization, as a number of contextual and security concerns must be balanced before making such decisions.

Additionally, we have seen a growth in sites that aid developers with their practice such as the Q&A site StackOverflow [53], which is known to influence the practices of developers. A similar site has been created for sysadmins called SuperUser [19]. Future work should investigate these sites to better understand the issues that face sysadmins outwith the patching process, potentially by looking at the questions that these sites gather we can identify common issues faced and help to build tools that would aid in solving them. Furthermore, these tools should look to be collaborative both internally and externally, allowing admins to better perform the cooperative behaviours that they have been heavily linked to [28, 31, 60].

Our results suggest that Client sysadmins may be more likely to look to online communities, such as subreddits, for patch information regarding errors and post-installation issues compared to Server admins, possibly due to the wider availability of general client information which may be applicable to their client set-up. Through better understanding of these communities we may be able to identify how admins learn their security practices [46], potentially identifying security misconceptions similar to end-users [63]. Considering the level of support that communities provided in understanding a patch's risk [28], and the surprising survey results showing a lack of admins engaging with information on vulnerabilities, CVEs, and their criticality, future research should focus on how these are reported and presented to sysadmins. It appears that admins may attempt to apply patches based on severity of the vulnerability, other factors unique to their working context may out-weight the need for security.

Finally, our findings contribute to ongoing research into defining concepts such as the 'criticality' of a patch [51]. The online communities that sysadmins engage with provide insight into the sort of information that admins actually take into consideration when quantifying risks, such as patch quality. A holistic approach to vulnerabilities and patching may yield more actionable information for sysadmins as opposed to a scoring system that does not take into consideration the reality of patch management. Such a holistic approach also supports sysadmins in their 'broker' role [60]. Typically, sysadmins digest the technical information for their organizations into a rationale for action that best protects and suits their organization.

5.2 Testing may be ad-hoc

The testing of patches is a key stage in the patching process, with previous work indicating that use of staged deployment and dedicated test environments aid admins in identifying issues before they make their way into production systems. Our work indicates that these formal processes may not be as wide spread as previously thought. Only 37% of respondents indicated that they had test environments available, with the majority of testing apparently taking a much more informal and ad-hoc approach. One reason for this finding may be the fact that having a separate testing environment which accurately imitates a real production system will only result in doubling the workload of sysadmins as they must now maintain two distinct systems. Hence, a more streamlined approach is preferred, with many admins testing initially on their own personal machines or on of Virtual Machines. Future work should investigate these informal testing practices, which appear to be more prominent in SMEs, while larger organizations may have more resources available to set up and maintain dedicated testing environments and staged deployment techniques. Admins from large organizations were also more likely to identify patching policies as the reason for their approach than sysadmins from SMEs. This may be due to the fact that larger organization often have more matured procedures. Furthermore, vendors could aid admins by including information regarding the tests performed on patches before they were released. Doing so may alleviate some of the information searching admins must conduct. Early access schemes such as Microsoft's Security Update Validation Program [7] are also suitable ideas, allowing for reliability of patches to be tested in the wild, with the feedback quickly implemented before a wider release.

Despite less reliance on dedicated testing environments, sysadmins from SMEs are more likely to report that patches rarely cause errors. This may be due to the smaller size of SMEs, which may result in less complex systems with fewer additional programs and software, reducing the chances of potential conflict with newly introduced patches. Future work should investigate the role of these SMEs in discussions with vendors, since our results highlighted that many SMEs refrain from direct communication with vendors through use of tickets (23.3%; N=19) compared to their peers based within larger organizations (51.4%; N=71), identifying regular pain points and strategies to engage with vendors and gain their attention given that they may not be a priority.

5.3 Uninstalling is not default

One of the main aims of this survey was to expand upon the later stages of the patching process, in particular the troubleshooting

[6] https://en.wikipedia.org/wiki/Patch_Tuesday

[7] https://techcommunity.microsoft.com/t5/windows-it-pro-blog/what-is-the-security-update-validation-program/ba-p/275767

of errors. Previous studies identified that the most common response to a patch causing an error was to remove the offending patch [37, 54]. However in our survey, a large majority of sysadmins indicate that work is done to understand the scope and impact of an error first, with additional help coming from online forums or blogs. These strategies makes sense given the highly collaborative and problem solving nature of system administration [31]. Simply removing an error only delays an issue until the patch is fixed, often in the form of a hotfix [17] Additionally, sysadmins may be required to carry out their own internal investigation before or while attempting to gain help from online communities before requests for help may be considered. We found that admins may raise tickets with the vendors to get them to fix the issue, since when an error occurs the fault can either lie with the patch or the admin's specific system. What is interesting however is that limited number of admins from SMEs reported raising a ticket with vendors. Future work should aim to identify and expand on troubleshooting strategies outside of dedicated testing environments, which appear be prominent throughout all groups investigated.

5.4 Limitations

The responses from the survey participants are self-reported, and hence may not be reflective of actual behaviours due to social desirability bias [21]. Additionally, the channels for recruitment we used have been also been used in previous research [37, 39, 54], but to guard against potential invalid responses a simple attention check question was used in the survey. Although we performed a number of additional checks to ensure that our sample contained valid responses, there is no reliable method to validate our sample. This limitation was necessary as many of the moderators and admins of our chosen online communities and the security professionals we asked to share our survey explicitly asked for platform tracking to be removed due to the nature of our research as many of these platforms and the topics of discussion are highly linked to job security and performance.

While more than half the sample consists of North American respondents, findings are sufficiently similar to those of Tiefenau et al. [54], (predominantly European), and to those of Li et al. [37] (predominantly US) to allow some level of generalisation. However, the sample clearly skews towards Western developed nations, and regions with a vibrant IT sector such as South and East Asia are strongly underrepresented.

The overwhelming majority of admins we surveyed (86%) are male. Similar to previous work [31, 37, 39, 54], we did not manage to reach a sufficient number of sysadmins of different genders. Recent work has highlighted that non-cis male admins often have different working experiences within the male dominated workplace [10]. In some cases this situation requires non-male admins to perform additional work, forcing them to go above and beyond what is expected just to be viewed equally [33]. These differences likely impact all aspects of their work, potentially including patch management tasks and policy decisions within their organizations.

Finally, our questions regarding sysadmins' reliance on online sources are likely to be biased due to the fact that we directly recruited from such platforms, and therefore may not be reflective of the larger population of system administrators. In future work, alternative recruiting strategies should be emphasised that allow researchers to explicitly engage sysadmins with different levels of engagement with online platforms. Despite the difficulties in recruiting such groups [27, 34], there may be a potential solution to recruit from apprenticeship and training schemes [8] given the suitability of Computer Science students and their similarities to developers [52].

6 CONCLUSION

This paper has presented the results of a survey shared with 220 sysadmin from relevant patching communities of sysadmins and identifies the prominence, and impact of context on patching behaviours. We provide the research community with the largest sample of admins to date, giving us greater confidence in the results found. Analysis shows that there exists a number of differences in the approaches used by admins working for SMEs compared to large organizations indicating that factors, such as patching policies are more relevant in larger organization.

Additionally, we have expanded upon our understanding of testing set-ups used by sysadmins, with more informal approaches being more popular than previously anticipated. Finally, our work highlights that uninstalling offending patches is not the default option of many sysadmins and instead time and effort is placed in scoping the impact of errors, highlighting the problem solving nature of Patch Management, and the general practice of System Administration.

Finally, we found that there are sufficient similarities across system and organisation types that in-depth investigations into a specific sector, such as health care, [15, 17], are likely to be broadly generalizable to different sectors.

Since sysadmins actively use information from online communities in their patch management processes, we believe that future work should focus on creating a tool which systematically analyses patch-related discussions in a range of online communities and synthesises its findings in a way that is easy to understand and action for sysadmins from a broad range of backgrounds. Potentially a solution may exist which allows vendors to remain informed of their product and the issues and can create a beneficial relationship where online communities can aid vendors in fixing patch issues, while offering official workarounds that suit sysadmins' needs. Perhaps new software and techniques can be created to aid in the identification of troublesome patches and issues within one's system by utilising the wealth of online data that sysadmins generate regarding patching.

ACKNOWLEDGMENTS

The authors would like to extend a heartfelt thanks to all of the members and moderators of PatchManagement.org, and r/sysadmin who contributed to this survey. Additionally, we would like to thank the TULiPS Lab for all their support during this project.

REFERENCES

[1] Lawrence Abrams. 2020. Windows 10 KB4532693 Update Bug Hides User Data, Loads Wrong Profile. https://www.bleepingcomputer.com/news/microsoft/windows-10-kb4532693-update-bug-hides-user-data-loads-wrong-profile/

[8] https://www.learningpeople.com/uk/course/it-collections/systems-admin-collection/

[2] Kholoud Althobaiti, Adam D G Jenkins, and Kami Vaniea. 2021. A Case Study of Phishing Incident Response in an Educational Organization. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 338 (oct 2021), 32 pages. https://doi.org/10.1145/3476079

[3] John Bailey, Eser Kandogan, Eben Haber, and Paul P. Maglio. 2007. Activity-Based Management of IT Service Delivery. In *Proceedings of the 2007 Symposium on Computer Human Interaction for the Management of Information Technology* (Cambridge, Massachusetts) *(CHIMIT '07)*. Association for Computing Machinery, New York, NY, USA, 5–es. https://doi.org/10.1145/1234772.1234779

[4] R. Barrett. 2004. People and policies: transforming the human-computer partnership. In *Proceedings. Fifth IEEE International Workshop on Policies for Distributed Systems and Networks, 2004. POLICY 2004.* IEEE, Yorktown Heights, NY, USA, 111–114. https://doi.org/10.1109/POLICY.2004.1309157

[5] Rob Barrett, Yen-Yang Michael Chen, and Paul P. Maglio. 2003. System Administrators Are Users, Too: Designing Workspaces for Managing Internet-Scale Systems. In *CHI '03 Extended Abstracts on Human Factors in Computing Systems* (Ft. Lauderdale, Florida, USA) *(CHI EA '03)*. Association for Computing Machinery, New York, NY, USA, 1068–1069. https://doi.org/10.1145/765891.766152

[6] Rob Barrett, Eser Kandogan, Paul P. Maglio, Eben M. Haber, Leila A. Takayama, and Madhu Prabaker. 2004. 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* (Chicago, Illinois, USA) *(CSCW '04)*. Association for Computing Machinery, New York, NY, USA, 388–395. https://doi.org/10.1145/1031607.1031672

[7] Rob Barrett, Paul P Maglio, Eser Kandogan, and John Bailey. 2005. Usable autonomic computing systems: The system administrators' perspective. *Advanced Engineering Informatics* 19, 3 (2005), 213–221.

[8] Steve Beattie, Seth Arnold, Crispin Cowan, Perry Wagle, Chris Wright, and Adam Shostack. 2002. Timing the Application of Security Patches for Optimal Uptime. In *Proceedings of the 16th USENIX Conference on System Administration* (Philadelphia, PA) *(LISA '02)*. USENIX Association, USA, 233–242.

[9] Leyla Bilge and Tudor Dumitraş. 2012. Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security* (Raleigh, North Carolina, USA) *(CCS '12)*. Association for Computing Machinery, New York, NY, USA, 833–844. https://doi.org/10.1145/2382196.2382284

[10] Franziska Bumiller, Christian Eichenmüller, and Zinaida Benenson. 2023. "You're not smart enough for it. You can't do it anyway."-Experiences and Coping Strategies of Female System Administrators. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*. ACM New York, NY, USA, New York, NY, USA, 1–6.

[11] Caitlin Cassidy. 2022. Google outage: Tech giant apologises after software update causes search engine to go down. https://www.theguardian.com/technology/2022/aug/09/google-outage-search-down

[12] Olivier Crameri, Nikola Knezevic, Dejan Kostic, Ricardo Bianchini, and Willy Zwaenepoel. 2007. Staged deployment in mirage, an integrated software upgrade testing and distribution system. (2007), 221–236. https://doi.org/10.1145/1294261.1294283

[13] Stephanie de Smale, Rik van Dijk, Xander Bouwman, Jeroen van der Ham, and Michel van Eeten. 2023. No One Drinks From the Firehose: How Organizations Filter and Prioritize Vulnerability Information. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, 1980–1996. https://doi.org/10.1109/SP46215.2023.10179447

[14] Constanze Dietrich, Katharina Krombholz, Kevin Borgolte, and Tobias Fiebig. 2018. Investigating System Operators' Perspective on Security Misconfigurations. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (Toronto, Canada) *(CCS '18)*. Association for Computing Machinery, New York, NY, USA, 1272–1289. https://doi.org/10.1145/3243734.3243794

[15] Nesara Dissanayake, Asangi Jayatilaka, Mansooreh Zahedi, and M. Ali Babar. 2022. Software security patch management - A systematic literature review of challenges, approaches, tools and practices. *Information and Software Technology* 144 (2022), 106771. https://doi.org/10.1016/j.infsof.2021.106771

[16] Nesara Dissanayake, Mansooreh Zahedi, Asangi Jayatilaka, and Muhammad Ali Babar. 2021. A Grounded Theory of the Role of Coordination in Software Security Patch Management. In *Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering* (Athens, Greece) *(ESEC/FSE 2021)*. Association for Computing Machinery, New York, NY, USA, 793–805. https://doi.org/10.1145/3468264.3468595

[17] Nesara Dissanayake, Mansooreh Zahedi, Asangi Jayatilaka, and Muhammad Ali Babar. 2022. Why, How and Where of Delays in Software Security Patch Management: An Empirical Investigation in the Healthcare Sector. *Proc. ACM Hum.-Comput. Interact.* 6, CSCW2, Article 362 (nov 2022), 29 pages. https://doi.org/10.1145/3555087

[18] Thomas Duebendorfer and Stefan Frei. 2009. Why silent updates boost security. *TIK, ETH Zurich, Tech. Rep* 302 (2009), 98.

[19] Stack Exchange. 2023. SuperUser. https://superuser.com/.

[20] Sascha Fahl, Yasemin Acar, Henning Perl, and Matthew Smith. 2014. Why Eve and Mallory (Also) Love Webmasters: A Study on the Root Causes of SSL Misconfigurations. In *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security* (Kyoto, Japan) *(ASIA CCS '14)*. Association for Computing Machinery, New York, NY, USA, 507–512. https://doi.org/10.1145/2590296.2590341

[21] Robert J Fisher. 1993. Social desirability bias and the validity of indirect questioning. *Journal of consumer research* 20, 2 (1993), 303–315.

[22] Eben Haber and Eser Kandogan. 2007. Security administrators: A breed apart. *SOUPS USM* 3 (2007), 3–6.

[23] Eben M. Haber and John Bailey. 2007. Design Guidelines for System Administration Tools Developed through Ethnographic Field Studies. In *Proceedings of the 2007 Symposium on Computer Human Interaction for the Management of Information Technology* (Cambridge, Massachusetts) *(CHIMIT '07)*. Association for Computing Machinery, New York, NY, USA, 1–es. https://doi.org/10.1145/1234772.1234774

[24] Eben M Haber, Eser Kandogan, and Paul P Maglio. 2011. Collaboration in system administration. *Commun. ACM* 54, 1 (2011), 46–53.

[25] Dennis G. Hrebec and Michael Stiber. 2001. A Survey of System Administrator Mental Models and Situation Awareness. In *Proceedings of the 2001 ACM SIGCPR Conference on Computer Personnel Research* (San Diego, California, USA) *(SIGCPR '01)*. Association for Computing Machinery, New York, NY, USA, 166–172. https://doi.org/10.1145/371209.371231

[26] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "... No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices.. In *SOUPS*, Vol. 15. usenix, Ottawa, Canada, 1–20.

[27] Pooya Jaferian, Kirstie Hawkey, and Konstantin Beznosov. 2010. Challenges in evaluating complex IT security management systems. In *Symposium on Usable Privacy and Security (SOUPS)*. ACM, Redmond, WA, 6.

[28] Adam Jenkins, Pieris Kalligeros, Kami Vaniea, and Maria K. Wolters. 2020. "Anyone Else Seeing this Error?": Community, System Administrators, and Patch Information. In *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, Genoa, Italy, 105–119. https://doi.org/10.1109/EuroSP48549.2020.00015

[29] Adam Jenkins, Maria Wolters, and Kami Vaniea. 2023. To Patch, or not To Patch? That is the Question: A Case Study of System Administrators' Online Collaborative Behaviour. arXiv:2307.03609 [cs.HC]

[30] Eser Kandogan and Eben M Haber. 2005. *Security administration tools and practices*. O'Reilly Sebastopol, CA, CA, USA, 357–378.

[31] Eser Kandogan, Paul Maglio, and Eben Haber. 2012. *Taming information technology : lessons from studies of system administrators*. Oxford University Press, Oxford.

[32] Mannat Kaur, Simon Parkin, Marijn Janssen, and Tobias Fiebig. 2022. "I needed to solve their overwhelmness": How system administration work was affected by COVID-19. In *25th ACM Conference on Computer-Supported Cooperative Work and Social Computing*. ACM, ACM, Virtual, 30 pages.

[33] Mannat Kaur, Harshini Sri Ramulu, Yasemin Acar, and Tobias Fiebig. 2023. "Oh yes! over-preparing for meetings is my jam:)": The Gendered Experiences of System Administrators. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW1 (2023), 1–38.

[34] Andrew G Kotulic and Jan Guynes Clark. 2004. Why there aren't more information security research studies. *Information & Management* 41, 5 (2004), 597–607.

[35] Katharina Krombholz, Wilfried Mayer, Martin Schmiedecker, and Edgar Weippl. 2017. "I Have No Idea What i'm Doing": On the Usability of Deploying HTTPS. In *Proceedings of the 26th USENIX Conference on Security Symposium* (Vancouver, BC, Canada) *(SEC'17)*. USENIX Association, USA, 1339–1356.

[36] Frank Li and Vern Paxson. 2017. A Large-Scale Empirical Study of Security Patches. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (Dallas, Texas, USA) *(CCS '17)*. Association for Computing Machinery, New York, NY, USA, 2201–2215. https://doi.org/10.1145/3133956.3134072

[37] Frank Li, Lisa Rogers, Arunesh Mathur, Nathan Malkin, and Marshini Chetty. 2019. Keepers of the Machines: Examining How System Administrators Manage Software Updates. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS'19)*. USENIX Association, USA, 273–288.

[38] Paul P Maglio, Eser Kandogan, and Eben Haber. 2003. Distributed cognition and joint activity in collaborative problem solving. In *Proceedings of the Annual Meeting of the Cognitive Science Society*, Vol. 25. Wiley, NY, US, 758–763.

[39] Florin Martius and Christian Tiefenau. 2020. What does this Update do to my Systems?–An Analysis of the Importance of Update-Related Information to System Administrators. In *6th Workshop on Security Information Workers*. USENIX, New York, USA, 12.

[40] Peter Mell, Tiffany Bergeron, and Dave Henning. 2005. Creating a Patch and Vulnerability Management Program.

[41] Microsoft. No Date. https://answers.microsoft.com/

[42] Rene Millman. 2020. Microsoft 365 outage blamed on Botched Network Driver update. https://www.itpro.co.uk/cloud/microsoft-azure/357686/microsoft-365-outage-blamed-on-botched-network-driver-update

[43] David Moore, Colleen Shannon, and k claffy. 2002. Code-Red: A Case Study on the Spread and Victims of an Internet Worm. In *Proceedings of the 2nd ACM SIGCOMM*

Workshop on Internet Measurment (Marseille, France) *(IMW '02)*. Association for Computing Machinery, New York, NY, USA, 273–284. https://doi.org/10.1145/637201.637244

[44] NCSC. 2016. Vulnerability Management. https://www.ncsc.gov.uk/guidance/vulnerability-management.

[45] NCSC. 2022. Cyber Essentials. https://cyberessentials.online/cyber-essentials-patch-management-explained/.

[46] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2016. How I Learned to Be Secure: A Census-Representative Survey of Security Advice Sources and Behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (Vienna, Austria) *(CCS '16)*. Association for Computing Machinery, New York, NY, USA, 666–677. https://doi.org/10.1145/2976749.2978307

[47] Robert W Reeder, Iulia Ion, and Sunny Consolvo. 2017. 152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users. *IEEE Security & Privacy* 15, 05 (2017), 55–64.

[48] Omid Setayeshfar, Junghwan "John" Rhee, Chung Hwan Kim, and Kyu Hyung Lee. 2021. Find My Sloths: Automated Comparative Analysis of How Real Enterprise Computers Keep Up with the Software Update Races. In *Detection of Intrusions and Malware, and Vulnerability Assessment*, Leyla Bilge, Lorenzo Cavallaro, Giancarlo Pellegrino, and Nuno Neves (Eds.). Springer International Publishing, Cham, 215–236.

[49] Deepa Shivaram. 2021. Internet outage that crashed dozens of websites caused by software update. https://www.npr.org/2021/07/22/1019333663/internet-outage-dns

[50] Adam Shostack. 2003. Quantifying patch management. *Secure Business Quarterly* 3, 2 (2003), 1–4.

[51] Jonathan Spring, Eric Hatleback, Allen Householder, Art Manion, and Deana Shick. 2021. Time to Change the CVSS? *IEEE Security Privacy* 19, 2 (2021), 74–78. https://doi.org/10.1109/MSEC.2020.3044475

[52] Mohammad Tahaei and Kami Vaniea. 2022. Recruiting Participants With Programming Skills: A Comparison of Four Crowdsourcing Platforms and a CS Student Mailing List. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 590, 15 pages. https://doi.org/10.1145/3491102.3501957

[53] Mohammad Tahaei, Kami Vaniea, and Naomi Saphra. 2020. Understanding Privacy-Related Questions on Stack Overflow. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376768

[54] Christian Tiefenau, Maximilian Häring, Katharina Krombholz, and Emanuel Von Zezschwitz. 2020. Security, Availability, and Multiple Information Sources: Exploring Update Behavior of System Administrators. In *Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security (SOUPS'20)*. USENIX Association, USA, Article 14, 20 pages.

[55] Christian Tiefenau, Emanuel von Zezschwitz, Maximilian Häring, Katharina Krombholz, and Matthew Smith. 2019. A Usability Evaluation of Let's Encrypt and Certbot: Usable Security Done Right. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (London, United Kingdom) *(CCS '19)*. Association for Computing Machinery, New York, NY, USA, 1971–1988. https://doi.org/10.1145/3319535.3363220

[56] Kami Vaniea and Yasmeen Rashidi. 2016. Tales of Software Updates: The Process of Updating Software. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 3215–3226. https://doi.org/10.1145/2858036.2858303

[57] Nicole F. Velasquez and Alexandra Durcikova. 2008. Sysadmins and the Need for Verification Information. In *Proceedings of the 2nd ACM Symposium on Computer Human Interaction for Management of Information Technology* (San Diego, California) *(CHiMiT '08)*. Association for Computing Machinery, New York, NY, USA, Article 4, 8 pages. https://doi.org/10.1145/1477973.1477979

[58] Nicole F. Velasquez, Suzanne Weisband, and Alexandra Durcikova. 2008. Designing Tools for System Administrators: An Empirical Test of the Integrated User Satisfaction Model. In *Proceedings of the 22nd Conference on Large Installation System Administration Conference* (San Diego, California) *(LISA'08)*. USENIX Association, USA, 1–8.

[59] Nicole F. Velasquez and Suzanne P. Weisband. 2008. Work Practices of System Administrators: Implications for Tool Design. In *Proceedings of the 2nd ACM Symposium on Computer Human Interaction for Management of Information Technology* (San Diego, California) *(CHiMiT '08)*. Association for Computing Machinery, New York, NY, USA, Article 1, 10 pages. https://doi.org/10.1145/1477973.1477975

[60] Nicole F. Velasquez and Suzanne P. Weisband. 2009. System Administrators as Broker Technicians. In *Proceedings of the Symposium on Computer Human Interaction for the Management of Information Technology* (Baltimore, Maryland) *(CHiMiT '09)*. Association for Computing Machinery, New York, NY, USA, Article 1, 8 pages. https://doi.org/10.1145/1641587.1641588

[61] Pauli Virtanen, Ralf Gommers, Travis E. Oliphant, Matt Haberland, Tyler Reddy, David Cournapeau, Evgeni Burovski, Pearu Peterson, Warren Weckesser, Jonathan Bright, Stéfan J. van der Walt, Matthew Brett, Joshua Wilson, K. Jarrod Millman, Nikolay Mayorov, Andrew R. J. Nelson, Eric Jones, Robert Kern, Eric Larson, C J Carey, İlhan Polat, Yu Feng, Eric W. Moore, Jake VanderPlas, Denis Laxalde, Josef Perktold, Robert Cimrman, Ian Henriksen, E. A. Quintero, Charles R. Harris, Anne M. Archibald, Antônio H. Ribeiro, Fabian Pedregosa, Paul van Mulbregt, and SciPy 1.0 Contributors. 2020. SciPy 1.0: Fundamental Algorithms for Scientific Computing in Python. *Nature Methods* 17 (2020), 261–272. https://doi.org/10.1038/s41592-019-0686-2

[62] Artem Voronkov, Leonardo A. Martucci, and Stefan Lindskog. 2019. System Administrators Prefer Command Line Interfaces, Don't They? An Exploratory Study of Firewall Interfaces. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 259–271. https://www.usenix.org/conference/soups2019/presentation/voronkov

[63] Rick Wash. 2010. Folk Models of Home Computer Security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (Redmond, Washington, USA) *(SOUPS '10)*. Association for Computing Machinery, New York, NY, USA, Article 11, 16 pages. https://doi.org/10.1145/1837110.1837125

[64] Etienne Wenger. 1999. *Communities of practice: Learning, meaning, and identity*. Cambridge university press, Cambridge, UK.

[65] Tianyin Xu, Vineet Pandey, and Scott Klemmer. 2016. An HCI View of Configuration Problems. (2016).

[66] Tianyin Xu and Yuanyuan Zhou. 2015. Systems approaches to tackling configuration errors: A survey. *ACM Computing Surveys (CSUR)* 47, 4 (2015), 70.