The (Un)usual Suspects – Studying Reasons for Lacking Updates in WordPress

Maria Hellenthal*, Lena Gotsche*, Rafael Mrowczynski*, Sarah Kugel†, Michael Schilling*, and Ben Stock*
*CISPA Helmholtz Center for Information Security: {hellenthal, gotsche, mrowczynski, schilling, stock}@cispa.de
† Saarland University: kugel589@gmail.com

***Abstract*—The widespread use of Content Management Systems (CMS) like WordPress has made these systems attractive targets for adversaries, with the vulnerabilities in the code posing serious risks. Despite being the most effective way to reduce these risks, more than half of all CMS installations lack the latest security patches. Researchers have tried to notify website operators about vulnerabilities using vulnerability notifications, which often exhibit limited impact. In this paper, we use the Grounded Theory approach to investigate the reasons why website owners do not update their CMS. To gain a holistic view on lacking update behavior, we interviewed website owners with outdated WordPress-based systems as well as individuals involved in website creation and hosting. On the one hand, we could confirm issues known from other ecosystems, such as lack of risk awareness, perceived risks of updates, and update costs, as factors for lacking CMS updates. More importantly, our study identified factors that have not been explicitly addressed in the general updating behaviour and vulnerability notification literature: (1) the subjective value of a website to its owner and (2) the delegation of website operations, which influence updating behavior far more decisively. Furthermore, we showed that website owners perceive a potential compromise of their CMS only as a risk to themselves and not as a threat to the wider online community. These findings that we present as four non-update scenarios may partly explain the limited success of previous efforts to notify operators about vulnerabilities in their systems. Our study not only offers valuable insights for future research, testing the effectiveness of vulnerability notifications and studying updating behavior in general, but it also proposes practical suggestions on how to reduce the number of outdated systems on the web.**

I. Introduction

Content Management Systems (CMS) like WordPress (WP) are everywhere on the Web, and so are vulnerabilities in the code that run these systems. As with any vulnerability on the Web, those in CMS pose serious risks to website visitors (e.g., phishing), hosters (e.g., misuse of infrastructure), and also website owners (e.g., damaged reputations and even legal consequences). However, such vulnerabilities are particularly dangerous given that the widespread use of CMS allows highly automated exploitation on a multitude of different websites [11]. So far, the most effective way to reduce these risks is to keep systems up to date and thus eliminate all known vulnerabilities [14]. Nevertheless, recent data shows that more than half of the CMS installations in the wild lack the latest security patches [39]. A key reason for this might be the fact that - in one way or another - an action by the operators is needed to keep the site technically up to date. Either updates have to be initiated manually when required, or the automatic update function must be configured correctly (at least the automatic updates must not have been switched off intentionally). Given this fact, from a security perspective, it is of utmost importance to know the reasons why website owners (WOs) do not keep their websites up to date.

Although research has not yet directly addressed this question, findings from three related areas may provide some limited insights. One line of research has studied end users' perceptions and experiences regarding system updates but within the context of personal devices, like smartphones [31, 32, 41, 45]. Here, studies revealed diverse reasons for users' avoidance of system updates, like concerns about functional changes [41] and a lack of understanding the importance of security patches [15, 31]. Another research area has explored the reasons behind delays in updates by system administrators. It identified challenges such as the impact of organizational policies and culture [14, 40, 28] as well as a lack of skills and expertise needed for addressing complex patching tasks [40, 14].

While some of these findings may be transferable to website owners, there are some substantial differences between the context of personal devices and CMS, as well as between 'common' site owners and system administrators. For example, in contrast to the use of private devices, WOs are also (at least partly) responsible for the users of their websites. Compared to the typical website owner, system administrators are commonly acknowledged as 'IT experts', while many WOs share more characteristics with non-expert end-users. This distinction may imply a different perception of updates by site owners as compared to system administrators.

The third line of research studied ways to notify site owners when their systems are misconfigured, compromised, or even have actual vulnerabilities with so-called Vulnerability Notifications (VNs) [6, 7, 27, 35, 36]. These works demonstrated that such VNs can positively affect fix rates but that the efficacy depends on various technical [8, 36] and content-related

Network and Distributed System Security (NDSS) Symposium 2025
23 - 28 February 2025, San Diego, CA, USA
ISBN 979-8-9894372-8-3
https://dx.doi.org/10.14722/ndss.2025.23277
www.ndss-symposium.org

factors [8, 27, 43]. In the past, however, results on some of these factors have been inconclusive (e.g., regarding the type of sender [8]), and the effects tended to be rather low in general. Consequently, recent work has started to take a more WO-centered approach, which examines the receivers' perception of VNs [22, 29]. While these studies are an important first step to examine why WOs react to VNs as they do, they do not touch the more fundamental question: Why do website owners not patch their systems in the first place?

Our paper answers this question by using the Grounded Theory approach reflecting input from various parties involved in the life cycle of a website. Specifically, we triangulated data from interviews with WOs with outdated CMS and individuals involved in website creation as well as hosting. Our goal was to provide a holistic view of WOs' attitudes towards their sites and the difficulties and concerns they face with CMS updates.

Our results suggest that the reasons website owners avoid system updates are indeed in some aspects similar to those in the context of personal devices, like a lack of risk awareness and the perceived risks of updates. Notably, the latter factor also plays a role in the delays in patching observed among system administrators. However, we also identified previously unaccounted factors, specifically in the context of VNs, that can affect updating behavior far more decisively: (1) the subjective value of a website for a vulnerable WO, which is probably often much lower than previously assumed, (2) problems based on delegated website operations, such as responsibility diffusion and disabling effects, and (3) the lack of risk awareness regarding the impact on others. Even though previous studies on VNs indicated low fix rates [6, 7, 27, 35, 36], these factors were not specifically raised as reasons for non-fixing, which underscores our study's contribution to the field.

We present our findings in an explanatory framework of barriers preventing updates that serves to identify WOs that may be swayed to update. Based on these findings, we argue that there are multiple reasons at play when a WO does not update and that not all of these reasons can be influenced externally. Hence, no single communication strategy can ultimately reach satisfying clean-up rates for web vulnerabilities. Our findings do not only unlock valuable insights for future research, pushing the boundaries in testing the effectiveness of vulnerability notifications, but also spark considerations for researchers exploring update behavior in general.

II. Related Work

A. Updating Behavior

Keeping systems and software up to date is one of the primary mechanisms for end-users to enhance system security on personal devices [23, 41]. However, research has repeatedly shown that users often delay or even avoid updates [19, 30, 42, 41, 45]. Thus, researchers have examined the perceptions, attitudes, and behavior of individuals towards system updates and found that specifically non-expert users often fail to recognize security as a concern or a reason for updates [23, 47].

Related work explored in-depth why users avoid or delay installing software updates and discovered a variety of factors related to update risks, necessity, and costs [31]. Specifically, users mention reasons such as concerns about data loss [31, 41], unexpected functional issues or changes [41, 19, 30, 42, 16], the belief that their systems are functioning properly as they are [31, 42], and the time required [31, 30, 41] that keep them from updating their systems.

While non-expert users install updates less frequently compared to IT professionals [23], studies revealed that even experts do not always update, for instance, third-party libraries after first use [13] and cannot always deploy updates in a timely manner [28, 40, 4, 14]. However, in contrast to end-users who often seem to lack awareness of the link between updates and security, system administrators generally recognize the critical security nature of updates [24]. This distinction has been repeatedly highlighted, with IT experts rating software updates as an effective security measure [23, 33] while end users do not [23]. Instead, studies identify organizational-, people-, and technology-related factors, particularly within the context of system administration, contributing to delays in patching [14]. For instance, coordination issues [40, 14], capacity limitations in human resources [28, 14], and the complexity of patches [28, 14, 40] can all contribute to delays in the patching process.

Against this background, we made the initial assumption that WOs differ from personal device users and system administrators in their perception of updates, for instance, due to their responsibility for user security and often limited technical expertise. These differences require a tailored approach to understanding their behavior. Thus, we decided to investigate non-updating behavior of WOs using an exploratory research design inspired by Grounded Theory. While existing qualitative work on update behavior in other IT domains has mainly focused on isolated reasons for not updating [41, 19, 30, 40] (but see [14]), our study proposes four 'non-update scenarios' that explain the phenomenon under investigation in a more holistic way.

B. Vulnerability Notifications

With the constantly growing number of websites, the danger of security vulnerabilities on the Internet is also increasing. The question of whether large-scale security notifications (e.g., via email) increase vulnerability patching and clean-up of websites has been addressed by several quantitative studies (e.g., [6, 7, 26, 35, 36]). While these VNs do result in a statistically significant increase in fix rates, their impact is typically small (e.g., fix rate of 17% in notified versus 14% in control group [36]), with researchers encountering issues with reachability, mistrust in VNs, and a perceived lack of importance [8, 6, 35, 36, 29]. In light of this, several studies have attempted to tackle the technical hurdles and manipulated some of the factors that constitute trustworthy and convincing warnings like sender reputation, message framing, the amount of message detail, and suitable channels (e.g., email versus letter) [29, 36]. However, while any of these notifications turned out to be more effective compared to not notifying vulnerable parties at all, the impact of these factors remains unclear, as

none of these variables alone have significantly increased fix rates [22]. As a result of these unsatisfactory clean-up rates, recent work has started to take a different, operator-centered approach and focused on the receivers' perception and opinions about VNs [22, 29]. By using qualitative methods, researchers showed that recipients often mistrust the notifications and that they seek ways to verify 1) the sender of the message [22, 29], 2) their motivation to send the message, and 3) the existence of the vulnerability itself [22].

While these studies have shed light on the human-related factors affecting behavior towards vulnerability notifications, they do not examine the underlying reasons that prevent vulnerable WOs from patching their systems in the first place. Our study aims to fill this gap by exploring the circumstances that may be at play, such as factors that could critically impact a site owner's reaction to VNs.

III. Methods

The research question we pose in this work is: Why do many site owners not update their CMS? To answer this question, we employed a data-analysis strategy inspired by the Grounded Theory (GT) approach [20, 37, 9] that is best suited for an open exploration of the non-updating phenomenon without relying on a priori causal hypotheses. We interviewed website owners with outdated CMS (we call them *vulnerable WOs* in this paper) for a direct, first-person account of their website-maintenance practices in general and the reasons why CMS are not updated. However, as the internal perspective of such vulnerable WOs may not be free from systematic self-perception biases (i.e., self-serving tendencies), we expanded our data collection to include the perspective of website professionals, specifically those in hosting and website development. Given their experience with multiple site owners, these professionals possess an external bird's eye perspective on issues and decision-making aspects related to WO's non-updating behavior. We conducted a joint analysis of the interview data from both sources, using the method of data triangulation [12, 17] to draw a comprehensive picture of the phenomenon. This means that we used two different data sets generated and analyzed with the same methods (see Appendix A for more details on the GT approach and data triangulation).

A. General Study Procedure

We created two data sets: Data set 1 was collected through semi-structured interviews with 19 vulnerable website owners. Data set 2 consists of 9 semi-structured interviews with website professionals. In accordance with general recommendations in the methodological literature on semi-structured interviews [21, 48, 25], an interview guide was developed for each of the respective target groups (populations). The interview guides were partly adapted in the course of the data-gathering process to account for insights derived from previous interviews. This allowed for a more targeted exploration of topics relevant for answering our research question and is in line with the above-mentioned methodological recommendations regarding interviewing techniques in qualitative studies.

The interview guide for the vulnerable website owners focused on the following issues: (1) the significance of the website for the interviewees, (2) how their site was created, (3) any support they received with their website and the nature of such collaborations, (4) how they handle the ongoing maintenance and care of their site, (5) reasons for not updating their systems, and (6) their level of risk awareness (see Appendix B for the interview guide). The interview guide for the website professionals addressed the questions of (1) why, based on their experience, the interviewees believed that some website owners do not update their systems and (2) why they thought that some other site owners struggle to update their systems (see Appendices C and D for the interview guide). The interview guides served as a 'roadmap' for the interviewers but allowed for flexibility to tailor questions to the characteristics of each interviewee. Further, questions may have been added or omitted based on the flow of each individual interview.

The interviews were conducted via videotelephony between June 2020 and July 2023. We audio-recorded and transcribed them. As all of them were held in German, we translated the interview guides, code books, and verbatim quotations presented in this paper. Two pilot interviews preceded the actual interviews. These data were not included in the analysis due to potential bias towards security topics resulting from interviewing colleagues.

B. Data Set 1: Vulnerable Website Owners

We interviewed vulnerable WOs to collect firsthand experiences regarding the reasons behind the lack of CMS updates. Specifically, we targeted owners of WP-based websites, as WP is the most frequently used CMS deployed by professionals and lay persons alike (CMS market share of over 60%; [1]).

We conducted two rounds of interviews with vulnerable website owners. This approach aimed to address a potential limitation observed in the first round, where a random sampling procedure primarily resulted in interviews with WOs who assigned a low value to their sites. In order to ensure a good coverage of prevalent website types and to reach conceptual saturation [20], we coded a random sample of 2,000 outdated websites to identify website types occurring in the wild. Based on the results, we singled out websites with webshops for further investigation, assuming their potential for financial losses in a compromise makes them personally valuable to their owners. Thus, in the second round, we specifically targeted webshop owners to enhance our sample.

1) Sampling Round 1: We started our sampling of vulnerable WOs with a list of domains under the German top-level domain (.de) that resolved to an outdated WP version. We used the now-defunct `theinternetbackup.com` site as a starting point. Subsequently, we crawled each site (April 21-25 2021) and checked the HTML source for indicators of WP, e.g., links to a `wp-content` folder with version information in the URLs of the subresources. Of 10,660,865 .de domains that we initially checked, 1,008,290 were unique WP-based websites. Of these, 774,862 pages indicated a version number.

We defined outdated WP-based sites as systems that used a minor WP-version for which, at the time of the crawl, a (non-installed) minor update existed for six months or longer. For instance, we considered a website running WP version 4.9.7 outdated since the subsequent version 4.9.8 had been released more than three years before the crawl, the most recent WP version for this site would have been version 4.9.16. Further, we considered all systems older than version 3.7 as outdated, as WP ceased security updates for these versions. Ultimately, 184,571 (24%) of WP websites from our list were outdated.

Websites, and hence, WOs to be contacted were randomly sampled from the list. We only included websites and their owners in our final recruitment if (1) the WP version was still outdated at the time of compiling that list and (2) contact details including a German phone number were published. To avoid opt-in biases that can potentially occur by sending study invitations as a follow-up to email vulnerability notifications, we chose a direct phone contact strategy (cold-calling). We called the numbers of vulnerable WOs on the list one by one. In total, 482 WOs were contacted, of which 287 (59.5%) answered the call. Of these, 31 (10.8%) expressed interest in being interviewed. In the end, 13 WOs were successfully recruited and were interviewed in Sampling Round 1.

2) Manual Coding of Website Types: After analyzing the Sampling Round 1 data, it became evident that only five out of 13 interviewees expressed a sense of value towards their websites. In response, we aimed to ensure comprehensive coverage of reasons for not updating CMS by assessing whether we had interviewed WOs representing all typical use cases. To do this, we sought to identify the most relevant website categories prevalent in the wild. First, we conducted a new crawl of outdated WP-based sites, using the same method as described for Sampling Round 1 (May 9-19, 2023). This new crawl was necessary to address any potential gaps in use cases, as identifying missing scenarios would have required a new participant recruitment round with up-to-date website data. Then, we developed a preliminary code book containing website categories. We tested this code book on a random sample of 200 outdated WP-based sites, allowing for the addition of previously omitted categories. Last, three research assistants coded a randomly selected sample of 2,000 outdated websites using the final code book. Table I shows the identified categories and their respective frequencies within the sample.

3) Sampling Round 2: Our Round 1 sample covered the website type-categories 1 (ten cases), 3 (two cases), and 4 (one case) in Table I. We specifically deemed category 7, e-commerce sites, worthy of further investigation, due to the potential for financial losses associated with compromises, suggesting a higher value of the website (none of the Sampling Round 1 interviewees owned a webshop). We defined e-commerce websites as those having an implemented shop or appearing to host one but, upon closer examination, linked to a webshop on an external site. We chose not to distinguish between these two types because (1) our initial website inspection did not allow for definitive statements about the website's value based on this differentiation and (2) from a security standpoint, a compromise of the landing page that links to a webshop is still problematic for the WO (even if it does not necessarily affect the website visitor using the webshop). For participant recruitment in Sampling Round 2, we relied on the data obtained from the manual coding of websites. Specifically, we recruited six webshop owners from the 86 webshops identified in Table I by using the same cold-call strategy as described for Sampling Round 1.

TABLE I
RESULTS OF THE MANUAL CODING OF WEBSITE TYPES

	Website Categories	Count	Percentage
1	Business website	1152	58%
2	Other information platform/News blogs	146	7%
3	Website non-profit/club	137	7%
4	Personal/Hobby website	114	6%
5	Website under construction	114	6%
6	No judgement possible	100	5%
7	e-Commerce website	86	4%
8	Doesn't load/work	55	3%
9	Website public institution	34	2%
10	Other	34	2%
11	Transaction mediation service	28	1%

C. Data Set 2: Website Professionals

Data Set 2 consists of interviews with one hosting provider and eight web developers with CMS experience. We included members of these occupational groups, as their bird's eye perspectives provide an overall understanding of common problems and concerns related to the CMS updating process in a wide range of customers. While the hosting provider was recruited through personal contacts of one of the research team members, we contacted the web developers by posting ads in theme-specific forums, blogs, and groups on social networking platforms.

D. Data Analysis

All interview transcripts were initially coded in a bottom-up manner following the procedure of 'open coding' proposed by Grounded Theory [20, 37, 9]. At this stage, each data set was coded independently by two researchers. They identified discrete units of text relevant for our research question, created initial codes and subsequently discussed and adapted these codes to resolve interpretative divergences. Then, the same two researchers conducted several iterations of descriptive and axial coding [5] to thematically integrate open codes into groups and eventually build a system of increasingly abstract categories. The entire coding and categorization procedure was conducted separately for each of the two data sets due to their diverging perspectives. All coding was done using MAXQDA 2022 (VERBI Software, 2021) [44].

As a result of 'axial coding', we arrived at a set of six key categories grounded in more specific phenomena, which we found in our interview data at earlier stages of the analysis. Based on these categories that reflect in a nutshell the isolated factors responsible for non-updating behavior, we then identified four factor combinations, denoted in the paper as

'non-update scenarios' (see section IV.D). These combinations constitute our theory of how non-updating behavior can occur in different owners of WordPress-based websites.

During the analysis, we found that the participants' statements varied greatly within certain categories. An example of this would be the value of the website, which for some people was considered high, e.g., an e-commerce website, while for others the website had no value at all, e.g., an info website of a social club. These trends were used to characterize/define a category. For the most part, the interpretation of the responses did not pose any problems, as the participants expressed their thoughts very clearly. When a participant's statements were harder to interpret or conflicting, the researchers resolved the issues through discussions and by reviewing the broader context of a statement within a given interview.

We conducted interviews until our data analysis suggested saturation, meaning that all relevant aspects of the studied phenomenon and its categorical diversity had been thoroughly described and no new themes emerged from the data (note that this saturation was further confirmed by the webshop owner perspective in Data Set 1, which did not introduce new themes but enriched existing categories). In this context, we considered Data Set 1 (in the following: S_1) and Data Set 2 (S_2) as interconnected sources of information, forming a cohesive corpus of data. S_1 formed the core of our analysis. By using the method of targeted data triangulation [17, 12], we strategically employed S_2 to complement and enrich the categories that emerged from the analysis of S_1. By combining findings from the interviews with all 28 participants across both data sets, we achieved a point of conceptual saturation, ensuring comprehensive coverage of the studied phenomenon. [1]

E. Ethical Considerations

We kept basic demographic data as well as any personally identifiable information about interviewees, such as data recorded during the recruitment phase, strictly separate from the study data. Personally identifiable data were deleted after the data-gathering process had been completed. We used participant ID-numbers, password-protected sheets, as well as anonymized transcripts to ensure anonymity. Although our interviews were conducted via videotelephony, we only recorded audio-tracks of the conversations. We used these audio files for transcriptions and deleted them afterwards. All participants provided informed consent in advance of the study and were able to further acquire and verify information about our studies on dedicated websites. They received Amazon vouchers or compensation via bank transfer as a token of appreciation.

For our cold-call strategy (S_1) we followed a conservative version of the market research guidelines of the Market and Social Research Association in Germany [3] (e.g., we strictly followed guidelines such as calling between 9 am and 9 pm only). The responsible ERB for our institution reviewed and approved our study procedure.

[1] see https://osf.io/3hr68/ for a timeline of the entire study

IV. Results

In this section, we first present participants' demographic data from both data sets and some website-related information from S_1. We then describe the key analytical categories, including main sub-categories (where applicable) and their empirical substance from both data sets. Next, we present findings about the WOs' self-reported maintenance behavior and, last, discuss our findings in the context of barriers that prevent WOs from updating their CMS.

A. Participant Data and Website Information

Participants in S_1 (n = 19) were between 23 and 70 years old.[2] Eight participants were female and all others were male. Twelve participants had an academic degree and only two participants had not completed high school. Regarding the participants' websites, the majority (15) was used for commercial purposes. Ten were a web presence for small businesses, five were used as e-commerce platforms (four with an implemented webshop on the outdated WP-website and one linked to an external website), two were used as a web presence for a club or charity, and one was used as a private hobby blog. Participants' WP versions had been outdated between 0.5 and 8 years. We note that all but two WOs ran a WP version that was released at least a year before our interview. We also confirmed that all running versions had known vulnerabilities, yet only one ran a version before 3.7, i.e., all but one *could* have been upgraded within their respective branch. The demographic data of the participants as well as the information about their websites are listed in Table II.

Of the website professionals in S_2 (n = 9), one was a hosting provider (Noah) and eight were web developers. Participants were between 31 and 56 years old and all were male. Four participants had a university degree and three had a high school diploma. All but one web developer reported that they were IT professionals who earned their living through website work. The number of websites that they had created using a CMS ranged between 5 and 120. Detailed demographic information, as well as information about the participants' occupational backgrounds, can be found in Table III.

B. Findings

The inductive analysis of the transcripts from S_1 yielded six key categories, most of which were supported by the data from S_2. Each of these categories is based on a multi-level system of subordinate codes from which the key categories emerged (see Appendices E and F for the code books of S_1 and S_2).

At the highest level, we further grouped our key categories by the two general behavior change elements: motivation and ability - both inspired by various behavioral models (e.g., [18, 34, 10]). In line with these models, individuals must (1) be motivated to perform a certain behavior (e.g., updating) and (2) have the abilities (e.g., IT skills) to transform this motivation into successful action. This conceptual framework provides

[2] Please note that we only conducted a total of 18 interviews. One of them involved two interview partners simultaneously; see Sigrid and Tamara in Table II

TABLE II
DEMOGRAPHICS OF THE PARTICIPANTS AND WEBSITE INFORMATION IN S_1

Alias*	Age	Profession	Website Topic	Website Type	WP-Vers.**	Outdated for	CVEs	Max. CVSS score
Alexander (m)	33	Lawyer	Judiciary	Business	4.9.7	> 3 Years	27	9.8
Benjamin (m)	60	Engineer	Charity	Non-profit	5.1.3	> 2 Years	17	9.8
Christian (m)	64	Engineer	Consulting	Business	5.2.1	> 2.5 Years	27	9.8
Diana (f)	55	Tax consultant	Finance	Business	5.3.2	1.5 Years	14	6.6
Erik (m)	50	NA	Holiday	Personal/Hobby	5.4.2	> 1.5 Years	5	6.6
Fabienne (f)	70	Mediator, Lecturer	Consulting	Business	4.9.8	> 3 Years	27	9.8
Georg (m)	23	Web developer	Handicraft	Business	4.9.3	> 3.5 Years	33	9.8
Henry (m)	37	Carpenter	Handicraft	Business	4.8.1	> 4 Years	52	9.8
Isabelle (f)	58	PR Consultant	Marketing	Business	4.9.3	> 3 Years	33	9.8
Johannes (m)	52	General Manager	Handicraft	Business	3.6	> 8 Years	49	9.8
Katharina (f)	47	Designer, Architect	Marketing	Business	4.3.1	> 6 Years	82	9.8
Leon (m)	31	IT Project Manager	Charity	Non-profit	4.3.2	> 6 Years	81	9.8
Matthias (m)	37	Architect	Tourism	Business	5.2.9	> 0.5 Years	4	8.2
Niklas (m)	37	Musician	Music	e-commerce	6.0	1 Year	21	6.8
Olivia (f)	42	Management Assistant	Textiles	e-commerce	5.7.1	> 2 Years	32	8.6
Paula (f)	37	Online-Shop Owner	Foods	e-commerce	5.6.2	> 2 Years	34	8.6
Rainer (m)	55	Offset Printer	Car Accessories	e-commerce	4.9.6	5 Years	55	9.8
Sigrid (f)/Tamara (f)	64/59	Business Admin/Teacher	Gamification	e-commerce	5.3.12	> 0.5 Years	21	6.8

Note: *We assigned pseudonyms to the interviewees to preserve their anonymity. **Refers to the websites' WordPress version, its outdatedness in years, the number of CVEs, and their maximum CVSS score at the time of the interview.

TABLE III
DEMOGRAPHICS OF THE PARTICIPANTS IN S_2

Alias	Age	Highest Qual.	IT Expert	CMSs created	Website Maintenance
Noah (m)	N/A	N/A	Yes (Hoster)	N/A	N/A
Oliver (m)	31	Master Degree	Yes	>6	Prof., Private, Honorary
Peter (m)	35	Specialised High School Dipl.	Yes	40	Professional
Richard (m)	40	High School Dipl.	Yes	40	Professional
Sascha (m)	42	PhD	Yes	10	N/A
Thomas (m)	52	Master-level Diploma	No	100	Professional
Uwe (m)	34	Master Degree	Yes	5-10	Professional
Vincent (m)	56	Study Course	Yes	120	Professional, Private
Walter (m)	49	High School Dipl.	Yes	20	Professional

Note that the information about CMSs and website maintenance was not applicable in Noah's case, as he was the hosting provider.

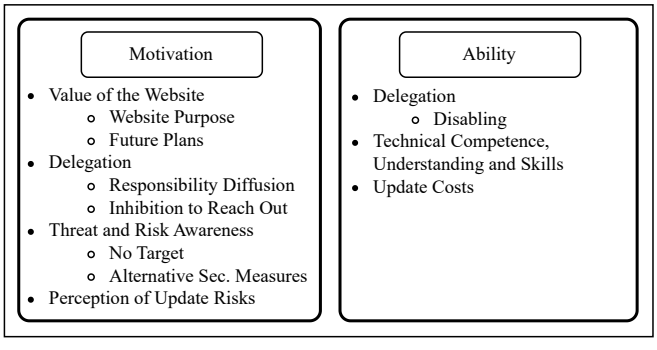

Fig. 1. Motivational and Ability-Related Key- and Sub-Categories

a more nuanced understanding of our six key categories that explain update behavior, since it describes their interplay in different individual cases of non-updating WOs. We present our categories in the order of importance, based on their impact on WOs' reported maintenance practices. In Figure 1, we list the identified key categories as well as their sub-categories accordingly under Motivation and Ability.

1) Value of the Website: The value of the website emerged as a key category from S_1. It appears to be one of the most significant factors influencing WOs' motivation to update. It is grounded in interviewees' answers to the explicit question of what the website means to them. Our results show that the value of a site varied greatly between interviewees. Contrary to our initial expectations, many interviewees (eight) reported that their website did not matter to them at all. Not surprisingly, a low website value reduces the motivation of its WO to engage in any updating activities. However, our sample also included 10 WOs who assessed the importance of their site as high or even very high. These cases pose a puzzle and require a further breakdown of the key category *Value of the Website* into its more detailed components (sub-categories) and integration of additional key categories into the explanatory frame. The key category *Value of the Website* summarizes two sub-categories:

Website purpose: The value of a website depended heavily on the purpose for which it was operated. In many cases, the websites were closely tied to the business activities of the respective WO. This suggests that the website would be considered important, as ten cases (Alexander, Fabienne, Georg,

Matthias, Niklas, Olivia, Paula, Rainer, Sigrid, Tamara; all S_1) indicate. These interviewees saw their site as a crucial tool for self-presentation, customer acquisition, and e-commerce. They believed any dysfunction of their website, be it from a cyber-attack or other technical issues, would significantly disrupt their business operations. Rainer (S_1), whose webshop presents the foundation of his business even described a potential site failure as a *"Super-GAU"* (German for worst-case scenario).

However, six interviewees who also operated their websites in a business context (Christian, Diana, Henry, Isabelle, Johannes, Katharina; all S_1) reported either little or no importance of their Internet presence. What all these individuals have in common is that they operate in markets where personal recommendations and serving a stable, long-term customer base constitute the predominant business model. As a result, they do not perceive their websites as particularly important tools for acquiring customers or clients, leading to neglect of these websites after their initial creation.

The perceived value of a website can change over time, as illustrated by the case of a club website owner, Leon (S_1). He reported that the value of the website had decreased significantly due to the rise of social-networking sites like Facebook. People interested in the club's activities were increasingly using these communication channels instead of the traditional website. Hence, while the value of the online presence remained relatively constant, the medium through which it was presented was changing, making the website less valuable to its owner.

Future plans: Future plans can also influence the value of a website. Two interviewees, both of whom used their websites for business purposes, reported plans to retire in the near future (Christian, Fabienne; all S_1). While Christian assessed the importance of his website for his business to be low, Fabienne considered her website to be a key tool for customer acquisition. Despite the website's importance to Fabienne and despite her awareness that her CMS was outdated, the prospect of retirement reduced her motivation to update. Here, the motivational factor of future plans helps to solve the puzzle of why a website with a high value remains outdated.

In S_2, the value of the website was hardly raised as an issue by the website professionals. The reason for this might be that web developers are primarily involved at the initial stages of a website's development but may not be as involved later on when the value of the website decreases, as we discovered in the interviews of S_1.

2) Delegation: The majority (15) of WOs in S_1 (except for Alexander, Erik, Georg, Leon) delegate some tasks to collaborators who provide, in some form, technical or content-related support for the creation and management of their websites. Analyzing these relationships, we identified four dimensions of delegation in S_1 and S_2 that can be best described by questions that probe the extent of:

- **Delegation pattern**: What is the fundamental structure of the delegation relationship? Is it between an individual WO and a tech-savvy friend or professional website agency or, in organizational settings, between employees?
- **Formalization degree**: Is the delegation primarily based on formal written contracts or less formal verbal agreements? Verbal agreements may often be perceived by the participants as a mutual exchange of favors rather than straightforward business transactions.
- **Coverage of delegation**: WOs can delegate website tasks, including content and technical aspects. Does the delegation include handing over all tasks to a supporting actor or only some specific activities?
- **Communication pattern**: Does the collaboration require the WO to initiate communication with the supporting actor, or does it involve proactive steps from the supporting actor, including maintenance without informing the WO?

At first glance, one might expect that delegations to supporting actors with a (presumably) higher website expertise would positively influence the website owners' updating practices. However, our data indicate that this assumption does not always hold true. Digging deeper into these dimensions, several problems crystallized that can make delegated website operation a source of non-updating behavior in its own right.

Responsibility Diffusion: Our data (S_1 and S_2) revealed that misunderstandings about who is responsible for hosting or maintaining a website can critically impact CMS updates. We refer to this phenomenon as "responsibility diffusion," a motivational category where the belief that another party is responsible for the technical maintenance or monitoring can lower or entirely cancel the WO's own motivation to act. Consequently, neither the site owner nor the external party performs the necessary updates. This can happen with individual WOs (Alexander, Diana, Johannes, Olivia, Paula; all S_1) and also with WO organizations (corporate entities that are website owners, as highlighted by Sascha; S_2).

The cases of Olivia and Paula (both S_1) indicate that responsibility diffusion can occur in informal and vaguely defined delegation relationships. While both website owners actively engage in the website's maintenance, they rely on friends and family for specific technical support. These collaborations are based on verbal arrangements and resemble an exchange of favors. For instance, Olivia's case involves favors within diffuse and multilayered familial relationships with her principal, the company owner. In contrast, Paula's collaboration involves a knowledge-for-goods barter relationship with a befriended IT expert, likely rooted in a shared ethical ideal (consuming organic food sold in Paula's webshop). Regarding delegation communication, these website owners actively need to contact their collaborators when facing technical difficulties. Proper monitoring and technical activities by the supporting actor occur only upon request. These circumstances contribute to misunderstandings, as exemplified by Paula's answer to the question why she has not updated her CMS for a while:

I think it's a misunderstanding between (name website professional) and me. He recently wanted to redo his server and asked me to wait with the update, and 'recently', probably means a little while ago. Well, thank you for bringing it up. I need to do that. I think I was waiting for a go-ahead from (name website professional) and haven't received it yet. I believe that was the reason (Paula).

A contrasting type of delegation became manifest in Rainer's case. He delegates all website-related activities to a website professional who actively informs him about the outdated status of his website. Despite being fully aware of the need for updates, Rainer, after having talked to the website professional, consciously decided not to perform updates. Instead, they chose to embark on the development of a new website to mitigate the potential risk of crashing the existing one. In this case, there is a clear understanding and agreement between Rainer and the expert regarding the technical maintenance and monitoring responsibilities. The decision to delay updates reflects a careful and strategic approach to ensure a smooth transition to the new website. In Rainer's case, no responsibility diffusion is present. Non-updating is a result of a conscious weighting of different risks - however flawed this result may appear from the point of view of web-security experts.

The data from S_2 reveals that responsibility diffusion can also occur in larger organizational settings within a different type of delegation pattern. The phenomenon arises in organizations with complex internal structures when members assume someone else is responsible for a specific task, resulting in inaction. This can be especially problematic when it comes to updating the CMS of the organization's website, as tasks may not be clearly defined or members may deliberately avoid taking on additional workload (e.g., updating the CMS when initially assigned to update website content). These challenges resulting from a lack of clarity in a delegation relationship contribute to the confusion surrounding responsibilities. This problem is described by Sascha (S_2):

... often someone is assigned to do content updates, such as regularly updating news etc.... But, how shall I say this, that they don't realize that nobody has been clearly assigned the responsibility to do the technical maintenance, and with this, I mean among others regular security updates (Sascha).

Disabling: Our data also revealed possible disabling effects resulting from occasional delegations of sophisticated technical activities to website professionals. This practice can lead to the emergence of increasingly complex technical solutions, often at the expense of usability and WO's agency. As a result, WOs who are still involved in the technical maintenance of their sites may encounter difficulties in understanding and running their websites on their own. As the complexity of technical solutions grows, WOs become more dependent on professionals, making it harder for them to comprehend the solutions and effectively operate their websites on the day-to-day level. This knowledge gap has implications for troubleshooting issues and making informed decisions about CMS updates. We consider disabling an ability-related theme, as the complex technical solutions make it more difficult for WOs to complete updates. The problem is exemplified by a comment of Niklas, a webshop owner, who wishes to return to simpler technical solutions:

[B]ut I think with the new version of the website, I will definitely involve him (befriended programmer). He actually created the WordPress theme, but I don't find it very practical. There are some issues; (...), and he uses a lot of Bootstrap. I don't really want to use Bootstrap either. I would prefer to leave out many plugins, eliminate excessive technology (Niklas).

Inhibition to reach out: We observed this motivational phenomenon in two interviews (Olivia, Paula; both $S1$), where WOs reported a hesitancy to seek assistance from website professionals who provided their services informally as favors, rather than under formal contracts. It appeared that participants were concerned that frequent requests for assistance might burden or inconvenience these individuals. This hesitancy highlights the complexities of navigating professional collaborations embedded in interpersonal relations. Olivia, who is required to contact the niece of her boss for help with technical problems, exemplifies this problem:

That's the thing when you approach them with a small question and... Yeah, they (website professional) get annoyed if they don't invoice for it (Olivia).

3) Threat and Risk Awareness: Threat and Risk Awareness emerged as a prominent theme in both data sets. It is a motivational category since one can assume that a higher threat and risk awareness motivates WOs to keep their CMS updated. Eight interviewees in S_1 (Alexander, Benjamin, Fabienne, Isabelle, Johannes, Rainer, Sigrid, Tamara) were not aware of any risks related to the outdatedness of their CMS. This fundamental misunderstanding was spread among participants with all degrees of website value from low to high. In cases of high website value (Alexander, Fabienne, Rainer, Sigrid, Tamara; all S_1), the lack of risk awareness can contribute to the explanation of why the respective CMS is not updated.

A vague risk awareness devoid of any specifics was found in seven transcripts (Diana, Erik, Georg, Leon, Matthias, Niklas, Paula; all S_1). Another three interviewees (Christian, Henry, Katharina; all S_1) were aware that their CMS are not up-to-date and that this fact can imply specific security risks. Recall that all versions ran by the interviewees at the time of the respective interview had known security vulnerabilities. While all three knowingly accepted these risks because their websites had low value for them, they merely looked at the dangers to themselves. None of them mentioned the possibility that compromised websites may be abused by attackers to launch attacks against *others*. Only when specifically asked about the potential risks to others, WOs with webshops in the last interview round expressed concerns, but these were limited to the personal data collected through their webshops. However, as exemplified in a recent study by Hennig et al. [22], attackers may abuse these compromised domains for various purposes, including SEO spam or hosting fake shops.

While Oliver (S_2) acknowledged that some website owners (his clients) are indeed aware of the risks associated with outdated CMS, five website professionals (Noah, Peter, Richard, Sascha, Vincent; all S_2) confirmed the role of lacking risk awareness and incomplete understandings of the risks in the issue of outdated systems. A further breakdown of the key category "Threat and Risk Awareness" reveals two sub-categories that can be described as website owners' "rationalisations" for their CMS' outdatedness.

No target: The lack of threat and risk awareness results from the belief that the consequences of an outdated system would be minor because nothing of value (e.g., sensitive information of others) can be gained from a website, as the statements of nine interviewees in S_1 (Benjamin, Christian, Fabienne, Leon, Matthias, Niklas, Olivia, Rainer, Sigrid) indicate. This phenomenon appeared in the statements of both non-risk-aware and (somewhat) risk-aware participants. For example, Fabienne (not aware of any risk) stated that she cannot imagine the risks of an outdated system being high, as her website only provides information and does not have interactive features such as a webshop. However, even four interviewees running webshops (Niklas, Olivia, Rainer, Sigrid) did not perceive the risks of outdatedness as high, as "there is not much to take" on their websites. Generally, this problem was also raised by three website professionals (Peter, Richard, Vincent; all S_2), who reported that some WOs do not perceive their websites as interesting or important enough for potential attackers, as stated by Peter:

> *People, or many customers, say, when I tell them we need to do an update, a security update, "I am just a dog groomer" or something, my website is not interesting for anyone (Peter).*

Noah (S_2) attributed the lack of understanding to website owners' perception that website security threats are limited to a few typical scenarios, such as spamming. This narrow view may prevent website owners from recognizing and understanding the broader range of possible attack scenarios, as illustrated by Peter (S_2):

> *This relationship, that automated attacks do not deal with the content of the website, but rather aim to access the capacities of the server, that it is actually completely irrelevant what is on the website, people simply want access to a foreign server to misuse it in some way. Therefore, a danger that is not consciously recognized by people (Peter).*

Alternative security measures: Another rationalisation made by five interviewees in S_1 relates to the alternative security measures they used to protect their website from potential harm. For instance, Benjamin, Christian, Georg, and Leon mentioned the regular backups, which would help to restore their websites with little effort. This again highlights the lack of understanding of the risk to others rather than to their own online presence.

4) Perception of Update Risks: The statements of 11 interviewees in S_1 (Alexander, Erik, Georg, Isabelle, Leon, Matthias, Niklas, Olivia, Rainer, Sigrid, Tamara) indicate that CMS updates are perceived as a source of risk. This assumption impacts update motivation in a negative way: Website owners avoid CMS updates due to the fear of possible website malfunctions. In this context, the interviews with Rainer, Sigrid, and Tamara indicate the problem of disregarding update notifications, as long as the system appears to work properly. This creates a delay in addressing potential issues and implementing necessary updates until the system's performance is negatively impacted, prompting action. This problem was brought up by Rainer in response to the request to elaborate on the specific reasons why his CMS is not up to date.

> *As I always say, never touch a running system. As long as something is working, I don't need to change it, and if it's working well, I don't need to change it. That's simply the reason (Rainer).*

While some participants (Alexander, Isabelle, Sigrid, Tamara; all S_1) raised more general worries about updates causing issues, others provided more specific insights. For instance Erik, Leon, Niklas and Rainer (all S_1) mentioned concerns about the impact of CMS updates on plugins and their complex structures. In particular, Niklas and Rainer, both webshop owners, share concerns about compatibility issues between plugins and CMS that may arise from updates, potentially impacting website functionality. Niklas, expressing concerns about the time-consuming nature of resolving issues caused by updates, opts to delay updates to allocate sufficient time for addressing them. Rainer's fear of the risks associated with updates led him to keep his CMS outdated for an extended period and eventually create a new website to circumvent the problem.

The issue of perceived update risks as update obstacles is also supported by observations of two interviewees in S_2 (Sascha and Richard), who highlighted that WOs might not update as they prioritize website functionality over security. This mindset is likely linked to the perception that potential functionality issues are more likely than an attack. This "selective perception", as Sascha called it, leads WOs to prioritize avoiding website disruptions caused by updates, rather than addressing security concerns, even though the latter may have more severe consequences in the long run.

Despite the limited size of the qualitative sample, it seems to be remarkable that most interviewees expressed concerns about the negative impact of updates on website functionality. Their fears of update-related dysfunctions contribute to the fact that they drag their feet on CMS updates.

5) Technical Competence, Understanding and Skills: Eight website owners (S_1) stated that they have limited to no IT knowledge (Alexander, Diana, Henry, Isabelle, Johannes, Rainer, Sigrid, Tamara). Johannes even revealed that he did not know what WP is. For some site owners, this lack of technical knowledge can present a challenge when updating their CMS.

The statements of three website professionals (Noah, Peter, Sascha; all S_2) shed light on a common problem regarding WOs' comprehension of the technical aspects involved in website maintenance. In particular lay WOs tend to only

consider the content-update aspect and overlook the continuous operational aspect that requires ongoing technical maintenance. This lack of understanding can result in websites being not properly maintained. On the other hand, three site owners (Erik, Georg, Leon; all S_1) reported having high levels of IT expertise and emphasized that they did not need external support in maintaining their sites. Georg develops websites as a profession, Leon holds a PhD in Computer Science, and Erik's experience in running computer centers for third parties gave him confidence in his technical abilities. However, neither of these jobs did require any specialized knowledge about CMS technology or website security in general, as the statement by Erik illustrates:

> *So I'm in my professional life, I run data centers with my team on behalf of clients. ... So I think I know roughly what I'm doing in this area. Ehm that's basically a by-product in terms of know-how, that I don't have to acquire any new knowledge at this point in order to run it. For the operation. In terms of content, how to do that in WordPress, yes. That's not my area of responsibility. I'm just active in the infrastructure, but technically it's not witchcraft to me (Erik).*

The cases of Erik, Leon and Georg draw attention to the problem that the absence of proper CMS maintenance is not always due to a lack of IT expertise. WOs with technical knowledge may neglect proper CMS maintenance due to other factors, such as the low importance of the websites for Erik and Leon. However, two website professionals (Richard and Sascha; S_2) noted that IT experts acting as WOs, such as IT administrators in organizational settings, may sometimes lack the specific knowledge and expertise needed to maintain applications like WP. This is highlighted by Sascha:

> *Well, the IT guy, and I myself am an IT guy, always speaks of several layers. One is the naked technical operation, where there must be a server, there must be storage, it must be backed up somehow, and that can be handled by the typical IT admin in companies. But then there is an application running on this infrastructure, in this case, the CMS, and this application must also be maintained, in terms of updates and so on. And often the IT people who kind of have that responsibility imposed on them, are familiar with the infrastructure layer, but not at all with the application layer (Sascha).*

Thus, our data indicate that the challenge of proper website maintenance may not be limited to IT-layperson website owners, but extends to site owners with technical knowledge as well. In some cases, IT professionals may neglect to update due to other factors such as low website value, and in other cases because they may lack specific CMS expertise.

6) Update Costs: The theme Update Cost was found to be prevalent in both data sets. It refers not only to the challenges faced by WOs in terms of time but also in terms of financial resources. Thus, in line with behavioral models like Fogg's [18], we consider this category as an ability-related barrier, as the lack of time and money makes it more difficult for individuals to complete a target behavior.

Five website owners (S_1), none of whom assessed the value of their website as particularly high, stated that the website and its maintenance simply did not have priority over other responsibilities (Henry, Isabelle, Johannes, Katharina, Leon).

Henry (S_1) seeks IT support for his website but lacks the necessary financial resources. He faces a conflict between investing in his website and other business areas, a problem that is raised by three website professionals (Richard, Thomas, Vincent; all S_2) as well. Some customers prioritize cost savings over the professional technical maintenance of their site and may choose to manage and operate the website themselves rather than paying for technical services offered by professionals. However, the cases of Niklas and Olivia (both S_1) show that opting for professional maintenance services is not always a choice. Both strongly desire more professional website assistance but face financial constraints. Olivia, for instance, cannot afford the high prices charged by professional agencies to maintain her webshop, exceeding her company's financial capabilities. Thus, she relies on assistance based on acquaintances' goodwill.

C. Self-reported Maintenance Behavior

While we know for a fact that the interviewed WOs (S_1) *all* used outdated WP systems at the time of contact, it is interesting to understand how they perceived their technical- and content-related effort. While 11 interviewees expressed awareness about their CMS's outdatedness, eight participants (Benjamin, Eric, Matthias, Niklas, Olivia, Paula, Sigrid, Tamara) lacked this clear awareness or admission. On the technical side, the majority of participants reported minimal updates to their websites and CMS. Only four WOs, who valued their websites, mentioned updating the PHP version at some point (Alexander, Benjamin) or regularly performing plug-in updates (Niklas, Paula). As for the website content, six interviewees stated that they regularly (Benjamin, Johannes, Niklas, Paula, Sigrid) or sporadically (Alexander) update it. Once again, all but one of them (Johannes) expressed some level of value for their website. Three participants (Fabienne, Christian, Leon) stated putting time, money, and effort into GDPR adjustments. While Katharina reported never having done a content update, as the information provided on the website remained relevant and unchanged over time, most interviewees admitted to neglect the website content.

Thus, many participants (S_1) admitted that they had neglected their website in terms of technical and/or content-related maintenance with only a few making adjustments they deemed absolutely necessary (e.g., GDPR adjustments that were mandated by the highly publicized legislation). This neglectful behavior can be seen as a result or symptom of the key categories presented above.

D. A Framework of Barriers Preventing Updates

Our data show that factors like the Value of the Website, Delegation, Threat and Risk Awareness, Technical Competence, the Perceived Risk of Updates, as well as Update Costs, can inhibit website owners' update behavior. Based on these findings, we propose an empirically grounded explanatory

framework encompassing the barriers and challenges faced by WOs operating their websites via a CMS. This framework constitutes the final outcome of our grounded-theoretical analysis. It also explicates the trade-offs involved when considering updates and offers insights into the decision-making, both conscious and unconscious. It outlines four non-update scenarios and ultimately allows us to identify site owners who may be swayed to update their CMS. [3] Within this framework a website's value is the most significant factor in determining update behavior for most WOs. Our data indicates the following four non-update scenarios:

Low Website Value

(1) Low Website Value and Inaction: When website owners perceive the website value to be low, this often leads to neglect and disregard in terms of content and technical maintenance, as their motivation to care for the website diminishes. While other factors may still have some influence on website owners' unconscious or conscious decisions to neglect their websites, our data suggest that a low website value tends to overshadow these factors, even if WOs possess risk awareness and/or technical skills.

High Website Value

When website owners place a high value on their websites, they demonstrate a strong motivation to keep their website up and running. However, various barriers can impede their CMS updates. At the core, these barriers often stem from their technical competence and ability to maintain the website themselves.

(2) Self-Reliance and Inaction: If site owners have confidence in their technical skills, and if they are able to manage the workload, they may proceed without external help. In these cases, factors such as lacking risk awareness or even the unawareness of missing updates can prevent them from taking action.

Conversely, if website owners lack technical skills, they are more likely to seek external support. The specific form of external support strongly depends on the Update Costs in relation to the financial resources of a WO or WO company.

Consequently, this support can range from partial to complete delegation of content-related and technical tasks.

(3) Full Delegation and Inaction: In cases of complete delegation, our data indicate that even with such full-service agreements, the perception of update risks can still result in an outdated CMS, as WOs may consciously avoid updates altogether to avoid an assumed possibility of disfunctionalizing or damaging their sites.

(4) Partial Delegation and Inaction: Partial delegation can lead to occasional support and is often embedded in informal interpersonal relations. This reliance on informal arrangements can result in issues such as responsibility diffusion, disabling effects, and hesitancy to seek support, all of which contribute to outdated CMS. While a lack of risk awareness and fear of website damage may also hinder WOs from taking action or addressing the situation, our findings suggest that these issues have comparatively less significance in these delegation-related circumstances.

[3] see https://osf.io/3hr68/ for a detailed classification of all participants into these non-update scenarios, along with the inhibiting factors within the six key categories described above.

V. Discussion

We first review our key categories in the context of previous research on general update behavior. We then discuss our novel findings regarding barriers that prevent CMS updates and how this impacts VN research. Next, we discuss the implications of our findings for the industry, and last, we present our study's limitations and suggestions for future research.

A. Comparison to Previous Research

Our research admittedly identified some similar factors responsible for the lack of CMS updates as those found in the literature on other types of updating behavior. Just like device users who often fail to recognize security as a concern or reason to update [23, 47], many website owners in our study were not aware of the security-related risks associated with their outdated CMS. In this context, WOs often did not perceive their websites as interesting or valuable enough to be targeted by hackers, a finding that mirrors observations in the context of personal devices, where participants believed that hackers only go after the 'big fish' [46]. Further, similar to users of personal devices, who shy away from updates out of fear of functional breakage or changes [41, 19, 30, 42], our interviewees saw updates as a potential threat to their sites' functionality. In a WO context, many participants specifically expressed concerns that incompatibilities with plug-ins used would disfunctionalize their websites, even though most participants never had any serious negative consequences or experiences. This observation is echoed in the system administrator literature, indicating that challenges arise with faulty patches and configuring patch dependencies, often resulting in breakdowns during the patch deployment process [24, 40, 14].

We also found the impact of technical expertise on updates confirmed [23], with some WOs explicitly stating that their lack of technical knowledge presents a challenge with CMS updates. Surprisingly, we did not only observe lacking update behaviour among laypersons but also among some IT experts. These findings reflect patterns noticed in previous research, showing that system administrators sometimes delay updates due to a lack of technical skills and expertise for handling complex patching tasks [28, 40, 4, 14]. We can also confirm the impact of update costs, such as the time required for updates, in hindering users from updating [31, 30, 41]. However, the financial constraints on hiring professional website support played an even higher role for some of our WOs. It is a factor that seems to be barely relevant in a personal device context.

Further, our research findings draw parallels to studies that have identified how unclear responsibilities about general

updates can lead to delayed updates [14, 2]. While previous studies focused on this phenomenon in organizational settings, one study explored a similar concept of responsibility diffusion in the context of privacy misconfigurations among WOs and situated this phenomenon within the broader context of delegation-related circumstances [38]. However, we substantially extend these findings by exploring different delegation dimensions that not only encompass responsibility diffusion but also other issues, such as disabling effects.

Our analysis also revealed factors expanding the general update behavior literature. These include low website value, delegation-related issues (such as disabling effects and inhibitions to reach out), and a lack of risk awareness regarding the impact on others. These factors have not been explicitly addressed as barriers to updates in the updating-behavior literature [41, 19, 30]. However, we do not imply that these newly-identified factors are exclusively specific to the CMS-updating context. For instance, users' general updating behavior on personal devices, such as mobile phones, may also be influenced by the perceived value of the device. While the context of managing websites often differs from personal devices, because CMS of abandoned websites can remain active for years or maybe even for decades while abandoned personal devices usually stop working due to the lack of electric energy within hours or days, there can still be parallels in terms of the potential risks involved. A personal device used for work purposes might store sensitive business data or connect to an internal network, raising concerns about potential security vulnerabilities and their impact on the overall system. This highlights the need for researchers to consider these factors when studying other types of updating.

To conclude, while certain findings indicate general problems in software update behavior, our study revealed both shared and potentially distinctive factors influencing update behavior among WOs compared to users of personal devices and system administrators. Recognizing these contextual distinctions is essential for developing effective solutions to address outdated CMS and systems in general.

B. Implications for Risk Communication

Our results suggest that not merely one, but rather several of our six factors combined explain why a website owner does not update their system. Previous research on vulnerability notifications has aimed to overcome some of these barriers, such as lack of risk awareness and lack of technical skills, by providing additional information to WOs. Some studies suggest that more detailed reports as well as technical support can increase clean-up rates somewhat [8, 26]. However, general fix rates in these studies are low, raising the question of whether other factors not yet considered are at play.

Our study suggests to avoid an isolated approach to addressing these factors. Instead, it underscores the importance of considering them as constellations/scenarios of barriers that impede website owners from performing updates. Further, our study emphasizes the need for addressing overlooked barriers when developing notification strategies and the content of notification messages. These barriers include low website value, issues related to delegation, and lacking risk awareness concerning potential dangers to others.

Based on our data, it becomes evident that website value stands as the most influential factor determining whether a website owner will be inclined to perform updates. Website owners who value their websites demonstrate a stronger motivation to maintain their online presence, suggesting that they are more likely to react to vulnerability notifications. In some cases, WOs consciously choose not to have external support for their websites, either because they believe their skills and knowledge are sufficient or due to financial constraints. In such situations, vulnerability notifications that effectively highlight the risks of outdated CMS may encourage these WOs to either update their websites themselves or reconsider their decision and allocate resources for external support.

For website owners who do have support, potential issues resulting from partial delegation need to be adequately addressed. One such concern is responsibility diffusion, where WOs who do not feel accountable for the technical maintenance of their website may ignore the content of notifications and consequently neglect CMS updates. To combat this issue, vulnerability notifications should clearly communicate the WO's role and accountability in maintaining the security of their site. This could be reinforced by including information obtained from the website's imprint or secondary sources, such as the hosting provider or web designer, to emphasize that the ultimate responsibility for updating their CMS lies with the site owner. As a lack of risk awareness and perceived update risks might indeed contribute to outdated CMS in these cases, effective risk communication and help for fixing the issue should complement such messages.

In certain instances, website owners may choose not to update their websites, even when they have complete website support or believe to possess the necessary technical skills and full awareness of their outdated CMS. For these WOs, the decision not to update could be a conscious assessment of the various risks or problems that could arise from updates compared to the risks of remaining outdated. Convincing these WOs to update may prove challenging. However, effective risk communication remains the most promising approach to motivate them to take action.

In regard to effective risk communication, our data shows that all website owners see the potential problems of CMS outdatedness in an 'ego-centric" manner: Those who perceived a lack of updates as a potential source of risk at all assumed that they would be the only person affected if a security breach actually occurred on their site. When not specifically cued, not a single interviewee mentioned the possibility that their vulnerable CMS could become a *source* of attacks. This suggests that future vulnerability notification campaigns should include passages highlighting the potential public risks of outdated CMS.

On the flip side, our data indicate that many vulnerable WOs care little about their websites. This presents a critical issue, as WOs who undervalue their sites seem to lack the necessary

motivation to update. This may lead to non-responsiveness to update notifications and other prompts. Given that the subjective value of a site can hardly be influenced externally, even the best-crafted VN addressing risks and technical help might fail. This may partly explain the low fix rates in previous research and highlights the need for alternative measures to reduce the number of vulnerable CMS.

C. Implications for Industry

People tend to lose interest in things over time. The same goes for websites: Once created with significant effort, many of them are eventually left abandoned. Such websites continue to exist on the Internet, and their vulnerabilities can pose a threat to visitors, hosters, operators, and the general public. Current CMS do not provide a solution to the problem of these 'abandoned' websites. While there are safer alternatives, such as static site generators, they are not as user-friendly as popular CMS such as WP. In light of these problems, it would be important for the CMS industry to adapt their products by offering systems that are just as user-friendly but generate static HTML websites by default. Hosting providers could support this initiative by offering services and tools that facilitate converting dynamic websites to static ones, enabling seamless transitions. At the very least, CMS and hosting providers should ensure layperson-friendly risk communication when websites are created or when automatic updates are switched off, educating users about the importance of keeping websites up-to-date.

Further, collaborative educational initiatives, involving governmental institutions, CMS and hosting providers, web development organizations, and cybersecurity experts, could be considered to enhance user knowledge on maintaining secure websites. For instance, public-recognition programs could serve to highlight websites and organizations that demonstrate exemplary security practices. This approach not only encourages website security measures but also raises public awareness about the importance of website security.

D. Limitations and Further Research

To address our study's limitations and guide future research, we outline several key considerations. First, we focused on WordPress, as WP is by far the most widely used CMS and should therefore provide a very representative insight. We believe that the issues we encountered with non-updates in WP are likely to be prevalent in other comparable CMS due to shared fundamental principles and functionalities across various CMS. Nevertheless future research should explore potential differences across different CMS platforms.

Second, as our main focus was on collecting and analyzing data in the highest quality possible, we deliberately chose to concentrate on the native language (German) context of the researchers. The adoption of a cold call strategy, coupled with the need for highly nuanced data evaluation, would otherwise have been challenging. Although we assume that the motives and attitudes of German speakers do not significantly differ from, for example, US speakers, future research should explore diverse cultural contexts.

Third, besides the security vulnerabilities studied here, which arise from outdated WP versions, unpatched plugins can also heavily impact the security of CMS platforms [39]. We believe that both types of lacking updates may stem from similar behavioral tendencies and be explained by the same models. We chose to concentrate on outdated CMS to maximize our sample size and participant diversity. Future research should explore unpatched plugins for a more comprehensive understanding of CMS security issues.

Fourth, we want to point out that S_1 might be biased towards webmasters operating business websites with phone numbers published on their imprints, as we exclusively contacted them via phone. Although our sample includes a 'hobby'-website as well, this means that more casual websites that do not publish such information are likely to be under-represented in our sample. To address this issue, future studies should explore the adoption of multiple contact approaches (e.g., phone and email) in their recruiting strategy.

Additionally, while we acknowledge that our study may be subject to some further biases such as opt-in biases, demand effects and social desirability bias, we made a conscious effort to minimize their impact. For instance, unlike previous studies such as [22], we avoided linking our recruitment approach to participants who had received VNs from authorities before. Instead, we opted for a more laborious cold call strategy. Also, we refrained from mentioning outdated CMS during recruitment. This aimed to create an open mindset during the interviews, reducing socially desirable behavior or priming effects related to recent contact with security topics.

To gain a deeper understanding of the barriers to updating, future work should contrast the perspectives of vulnerable WOs with those who regularly update. Furthermore, future research should use quantitative approaches to assess the prevalence of half-abandoned, low-value websites in order to identify cases where VNs are likely to be effective. This could be done by identifying and testing proxies for the website owners' value of the site, such as the last update, the frequency of content updates to the website, or the presence of dead links. In any case, we see a need for additional studies on marginal, abandoned and rarely visited websites as a complementary effort in large-scale web-security studies that so far has been strongly focused on most-frequently visited domains [36, 35]. Further, researchers should experimentally test the effects of other motivational and ability-related factors, such as diffusion of responsibility, lack of risk awareness, and lack of technical skills as a function of website value. These factors could be tested both in isolation and in different combinations to gain a deeper understanding of their effects on updating behavior and to develop more effective vulnerability notification strategies.

VI. Conclusion

The Web's overall security is threatened by thousands of outdated applications ripe for attackers to compromise. In this paper, we investigated the reasons for lacking updates in WP

instances through an interview study with two different populations: vulnerable website owners and website professionals. As a result of our data analysis inspired by the Grounded Theory approach, we identified six key categories that influence website owners' update behavior. In addition to the well-known factors such as lack of risk understanding, perceived risks of updates, technical limitations, and update costs, we identify and explore factors previously not specifically addressed in the updating behavior literature. These include the perceived value of the website, issues related to delegation-based operations, and a lack of awareness regarding potential risks to others, all of which significantly impact site owners' update behavior.

Our data indicate that many website owners attach very little value to their websites, which poses a challenge not only to researchers studying update behavior in other contexts, but also to those investigating the effectiveness of vulnerability notifications. Given that the value of the website is difficult to influence externally, even the best-designed VNs may not prompt these site owners to update. We have further conceptualized our key categories as four combinations that constitute empirically grounded 'non-updating scenarios' that serve to identify WOs that may be swayed to update their CMS when appropriately warned.

We conclude that the ease of setting up a CMS (e.g., WP) might be a double-edged sword. On the positive side, it facilitates content sharing for non-technical users. However, maintaining long-term security and functionality still requires a certain level of technical expertise and attention, which, when lacking, can have a negative impact on the Internet's security as a whole, but also on the legal certainty of the website owners. Addressing the issue of outdated or even abandoned websites requires proactive steps from CMS providers focusing on user-friendly, secure solutions like static-site generators, alongside implementing effective risk communication strategies. Moreover, collaborative efforts involving governmental bodies, CMS providers, and cybersecurity experts are crucial to educate users and enhance website-security practices through public recognition programs. These actions can mitigate the risks posed by outdated websites and foster a more resilient and secure online environment.

References

[1] "Usage statistics and market share of wordpress," 2023. [Online]. Available: https://w3techs.com/technologies/overview/content_management

[2] H. Assal and S. Chiasson, "Security in the software development lifecycle," in *Proceedings of the Fourteenth Symposium on Usable Privacy and Security*, Baltimore, MD, USA, 2018.

[3] Berufsverband Deutscher Markt- und Sozialforscher, "Richtlinie für telefonische befragungen," 2021. [Online]. Available: https://www.bvm.org/fileadmin/user_upload/Verbandsdokumente/Standesregeln_RL_neu_2021/Richtlinie_Telefonische_Befragungen_2021.pdf

[4] T. Bondar, H. Assal, and A. Abdou, "Why do internet devices remain vulnerable? a survey with system administrators," in *Proceedings 2023 Workshop on Measurements, Attacks, and Defenses for the Web*. San Diego, CA, USA: Internet Society, 2023. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2023/02/madweb2023-23043-paper.pdf

[5] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, Jan. 2006. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1191/1478088706qp063oa

[6] O. Cetin, C. Ganan, M. Korczynski, and M. van Eeten, "Make Notifications Great Again: Learning How to Notify in the Age of Large-Scale Vulnerability Scanning," in *Workshop on the Economics of Information Security (WEIS). 2017.*, San Diego, CA, Jul. 2017. [Online]. Available: http://www.infosecon.net/workshop/downloads/2017/pdf/Make_Notifications_Great_Again:_Learning_How_to_Notify_in_the_Age_of_Large-Scale_Vulnerability_Scanning.pdf

[7] O. Cetin, C. Ganan, L. Altena, T. Kasama, D. Inoue, K. Tamiya, Y. Tie, K. Yoshioka, and M. van Eeten, "Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai," in *Proceedings 2019 Network and Distributed System Security Symposium*. San Diego, CA: Internet Society, 2019. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_02B-2_Cetin_paper.pdf

[8] O. Cetin, M. Hanif Jhaveri, C. Gañán, M. van Eeten, and T. Moore, "Understanding the role of sender reputation in abuse reporting and cleanup," *Journal of Cybersecurity*, vol. 2, no. 1, pp. 83–98, Dec. 2016. [Online]. Available: https://academic.oup.com/cybersecurity/article-lookup/doi/10.1093/cybsec/tyw005

[9] K. C. Charmaz, *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis*. Thousand Oaks, Calif.: Sage, 2006.

[10] M. Conner, Ed., *Predicting health behaviour: research and practice with social cognition models*, 2nd ed. Maidenhead: Open Univ. Press, 2009.

[11] C. A. Conţu, E. C. Popovici, O. Fratu, and M. G. Berceanu, "Security issues in most popular content management systems," in *2016 International Conference on Communications (COMM)*. IEEE, 2016, pp. 277–280.

[12] N. K. Denzin, "Triangulation 2.0," *Journal of Mixed Methods Research*, vol. 6, no. 2, pp. 80–88, 2012.

[13] E. Derr, S. Bugiel, S. Fahl, Y. Acar, and M. Backes, "Keep me Updated: An Empirical Study of Third-Party Library Updatability on Android," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. Dallas Texas USA: ACM, Oct. 2017, pp. 2187–2200. [Online]. Available: https://dl.acm.org/doi/10.1145/3133956.3134059

[14] N. Dissanayake, M. Zahedi, A. Jayatilaka, and M. A. Babar, "Why, how and where of delays in software security patch management: An empirical investigation in

the healthcare sector," *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, no. CSCW2, p. 1–29, Nov 2022, arXiv:2202.09016 [cs].

[15] M. Fagan and M. M. H. Khan, "Why Do They Do What They Do?: A Study of What Motivates Users to (Not) Follow Computer Security Advice," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. Denver, CO: USENIX Association, Jun. 2016, pp. 59–75. [Online]. Available: https://www.usenix.org/conference/soups2016/technical-sessions/presentation/fagan

[16] M. Fassl, M. Neumayr, O. Schedler, and K. Krombholz, "Transferring Update Behavior from Smartphones to Smart Consumer Devices," in *Computer Security. ESORICS 2021 International Workshops*, S. Katsikas, C. Lambrinoudakis, N. Cuppens, J. Mylopoulos, C. Kalloniatis, W. Meng, S. Furnell, F. Pallas, J. Pohle, M. A. Sasse, H. Abie, S. Ranise, L. Verderame, E. Cambiaso, J. Maestre Vidal, and M. A. Sotelo Monge, Eds. Cham: Springer International Publishing, 2022, vol. 13106, pp. 357–383, series Title: Lecture Notes in Computer Science. [Online]. Available: https://link.springer.com/10.1007/978-3-030-95484-0_21

[17] U. Flick, "Triangulation in data collection," in *The SAGE Handbook of Qualitative Data Collection*, U. Flick, Ed. Thousand Oaks and London: Sage Publications, 2018, pp. 527–544.

[18] B. Fogg, "A behavior model for persuasive design," in *Proceedings of the 4th International Conference on Persuasive Technology - Persuasive '09*. ACM Press, 2009, p. 1. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1541948.1541999

[19] A. Forget, S. Pearman, J. Thomas, A. Acquisti, N. Christin, L. F. Cranor, S. Egelman, M. Harbach, and R. Telang, "Do or Do Not, There Is No Try: User Engagement May Not Improve Security Outcomes," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. Denver, CO: USENIX Association, Jun. 2016, pp. 97–111. [Online]. Available: https://www.usenix.org/conference/soups2016/technical-sessions/presentation/forget

[20] B. G. Glaser and A. L. Strauss, *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago: Aldine Publishing Company, 1967.

[21] C. Helfferich, "Leitfaden- und experteninterviews," in *Handbuch Methoden der empirischen Sozialforschung*, N. Baur and J. Blasius, Eds. Wiesbaden: Springer VS, 2019, pp. 669–686.

[22] A. Hennig, F. Neusser, A. A. Pawelek, D. Herrmann, and P. Mayer, "Standing out among the daily spam: How to catch website owners' attention by means of vulnerability notifications," in *CHI Extended Abstracts*. New Orleans LA USA: ACM, Apr. 2022, pp. 1–8. [Online]. Available: https://dl.acm.org/doi/10.1145/3491101.3519847

[23] I. Ion, R. Reeder, and S. Consolvo, ""...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. Ottawa: USENIX Association, 2015, pp. 327–346, meeting Name: Large Installation System Administration Conference. [Online]. Available: https://www.usenix.org/conference/soups2015/proceedings/presentation/ion

[24] A. Jenkins, P. Kalligeros, K. Vaniea, and M. K. Wolters, ""anyone else seeing this error?": Community, system administrators, and patch information," in *2020 IEEE European Symposium on Security and Privacy (EuroS'I&'P)*. Genoa, Italy: IEEE, Sep. 2020, p. 105–119. [Online]. Available: https://ieeexplore.ieee.org/document/9230392/

[25] J. Lazar, J. H. Feng, and H. Hochheiser, *Research Methods in Human-Computer Interaction*, 2nd ed. Cambridge, MA: Morgan Kaufmann / Elsevier, 2017.

[26] F. Li, Z. Durumeric, J. Czyz, M. Karami, M. Bailey, D. McCoy, S. Savage, and V. Paxson, "You've Got Vulnerability: Exploring Effective Vulnerability Notifications," in *25th USENIX Security Symposium (USENIX Security 16)*. Austin, TX: USENIX Association, Aug. 2016, pp. 1033–1050. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/li

[27] F. Li, G. Ho, E. Kuan, Y. Niu, L. Ballard, K. Thomas, E. Bursztein, and V. Paxson, "Remedying Web Hijacking: Notification Effectiveness and Webmaster Comprehension," in *Proceedings of the 25th International Conference on World Wide Web*, Montréal Québec Canada, Apr. 2016. [Online]. Available: https://dl.acm.org/doi/10.1145/2872427.2883039

[28] F. Li, L. Rogers, A. Mathur, N. Malkin, and M. Chetty, "Keepers of the Machines: Examining How System Administrators Manage Software Updates," in *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. Santa Clara, CA: USENIX Association, 2019, pp. 273–288. [Online]. Available: https://www.usenix.org/conference/soups2019/presentation/li

[29] M. Maass, A. Stöver, H. Pridöhl, S. Bretthauer, D. Herrmann, M. Hollick, and I. Spiecker, "Effective Notification Campaigns on the Web: A Matter of Trust, Framing, and Support," in *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Aug. 2021, pp. 2489–2506. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/maass

[30] A. Mathur, J. Engel, S. Sobti, V. Chang, and M. Chetty, ""They Keep Coming Back Like Zombies": Improving Software Updating Interfaces," in *Twelfth Symposium on Usable Privacy and Security*. USENIX Association, 2016, pp. 43–58.

[31] A. Mathur, N. Malkin, M. Harbach, E. Peer, and S. Egelman, "Quantifying Users' Beliefs about Software Updates," in *Proceedings 2018 Workshop on Usable Security*. San Diego, CA: Internet Society, Feb. 2018. [Online]. Available: https://doi.org/10.14722%2Fusec.2018.23036

[32] P. Rajivan, E. Aharonov-Majar, and C. Gonzalez, "Update now or later? Effects of experience, cost, and risk preference on update decisions," *Journal of Cybersecurity*, vol. 6, no. 1, p. tyaa002, Jan. 2020. [Online]. Available: https://academic.oup.com/cybersecurity/article/doi/10.1093/cybsec/tyaa002/5788613

[33] R. W. Reeder, I. Ion, and S. Consolvo, "152 simple steps to stay safe online: Security advice for non-tech-savvy users," *IEEE Security & Privacy*, vol. 15, no. 5, pp. 55–64, 2017.

[34] R. Schwarzer, S. Lippke, and A. Luszczynska, "Mechanisms of health behavior change in persons with chronic illness or disability: The Health Action Process Approach (HAPA)." *Rehabilitation Psychology*, vol. 56, no. 3, pp. 161–170, 2011. [Online]. Available: http://doi.apa.org/getdoi.cfm?doi=10.1037/a0024509

[35] B. Stock, G. Pellegrino, C. Rossow, M. Johns, and M. Backes, "Hey, You Have a Problem: On the Feasibility of Large-Scale Web Vulnerability Notification," in *25th USENIX Security Symposium (USENIX Security 16)*. Austin, TX: USENIX Association, Aug. 2016, pp. 1015–1032. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/stock

[36] B. Stock, G. Pellegrino, F. Li, M. Backes, and C. Rossow, "Didn't You Hear Me? - Towards More Successful Web Vulnerability Notifications," in *Proceedings 2018 Network and Distributed System Security Symposium*. San Diego, CA: Internet Society, 2018. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018_01B-1_Stock_paper.pdf

[37] A. L. Strauss and J. M. Corbin, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, 3rd ed. Thousand Oaks, Calif.: Sage Publications, 2008.

[38] A. Stöver, N. Gerber, H. Pridöhl, M. Maass, S. Bretthauer, I. Spiecker Gen. Döhmann, M. Hollick, and D. Herrmann, "How website owners face privacy issues: Thematic analysis of responses from a covert notification study reveals diverse circumstances and challenges," *Proceedings on Privacy Enhancing Technologies*, vol. 2023, no. 2, p. 251–264, Apr 2023.

[39] Sucuri, "2021 Website Threat Research Report," Sucuri, Tech. Rep., 2021. [Online]. Available: https://sucuri.net/wp-content/uploads/2022/04/22-sucuri-2021-hacked-report.pdf

[40] C. Tiefenau, M. Häring, K. Krombholz, and E. von Zezschwitz, "Security, Availability, and Multiple Information Sources: Exploring Update Behavior of System Administrators," in *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, Aug. 2020, pp. 239–258, arXiv:2007.08875 [cs]. [Online]. Available: https://www.usenix.org/conference/soups2020/presentation/tiefenau

[41] K. Vaniea and Y. Rashidi, "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: ACM, May 2016, pp. 3215–3226. [Online]. Available: https://dl.acm.org/doi/10.1145/2858036.2858303

[42] K. E. Vaniea, E. Rader, and R. Wash, "Betrayed by updates: how negative experiences affect future security," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Toronto Ontario Canada: ACM, Apr. 2014, pp. 2671–2674. [Online]. Available: https://dl.acm.org/doi/10.1145/2556288.2557275

[43] M. Vasek and T. Moore, "Do malware reports expedite cleanup? An experimental study," in *5th Workshop on Cyber Security Experimentation and Test (CSET 12)*. Bellevue, WA: USENIX Association, Aug. 2012. [Online]. Available: https://www.usenix.org/conference/cset12/workshop-program/presentation/Vasek

[44] . VERBI Software, "Maxqda (2021)," 2022. [Online]. Available: https://www.maxqda.com/

[45] F. Vitale, J. McGrenere, A. Tabard, M. Beaudouin-Lafon, and W. E. Mackay, "High Costs and Small Benefits: A Field Study of How Users Experience Operating System Upgrades," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, May 2017. [Online]. Available: https://dl.acm.org/doi/10.1145/3025453.3025509

[46] R. Wash, "Folk models of home computer security," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*. Redmond Washington USA: ACM, Jul 2010, p. 1–16. [Online]. Available: https://dl.acm.org/doi/10.1145/1837110.1837125

[47] R. Wash and E. Rader, "Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, 2015, pp. 309–325.

[48] A. Witzel and H. Reiter, *The Problem-centered Interview: Principles and Practice*. Los Angeles et al.: Sage, 2012.

APPENDIX

A. Methodological background

Grounded Theory (GT): GT is a methodological approach to qualitative behavioral and social research (QBSR) that focuses on exploration and conceptualization of new or little-studied phenomena. It aims at an understanding that avoids an imposition of pre-existing interpretative patterns and theories on a studied phenomenon. Hence, GT is a set of methodological techniques that helps discovering and developing new conceptualizations through grounding generalizing interpretations of studied phenomena in the specifics of empirical data. It offers an epistemologically powerful alternative to 'armchair theorizing' that proposes explanations of social phenomena as logical constructs without any initial empirical underpinning. Of course, specific conceptualizations developed as results of studies implementing the GT methodology also have to be subjected to a rigorous testing that uses other quantitative, inferential-statistical or experimental methods, but their advantage is a

bigger likelihood of being adequate due to their initial empirical 'groundedness'.

The GT techniques include in particular a bottom-up coding strategy combined with writing of analytical memos that then become building blocks of publications (esp. their 'findings' sections). 'Coding' means here attaching descriptive/analytical labels to segments of primary data. GT researchers start this process with codes worded close to the specific content of data segments (quotations). This initial coding stage is called 'open coding'. After coding a significant part or all of the data material, these initial (quite detailed) codes are integrated into more abstract categories that become the major 'axes' of analysis. Hence this stage of analytical work is called 'axial coding'. Finally, most important and most abstract categories are identified (e.g., 'Technical competence, understanding and skills' in our study). These categories constitute the cornerstones of the resulting conceptualization. The entire process of coding, but especially its later stages, is supported by writing memos that explicate the meaning of individual categories (represented by higher-level codes) for answering the RQs.

The GT methodology also proposes a specific sampling procedure denoted as 'theoretical sampling'. Individual cases or units of observation (in our case individual website owners whom we interviewed) are selected step by step in alternation with the data analysis. The selection is driven by identification of gaps that remain open in the nascent conceptualization of the studied phenomenon. In other words, additional cases (units of observation) are chosen because their analysis promises further contributions to the conceptualization of a studied phenomenon. The process of additional case selection stops after data gathering turns out to result in no new conceptual insights. This is the point of 'theoretical saturation'.

The procedure of 'theoretical sampling', which we partly implemented in our present study, allows for modification of data-gathering instruments (like interview guides) as a research project progresses. Such modifications help to increase the accuracy of overall conceptualization by collecting more relevant and/or more targeted data as researchers acquire more detailed knowledge about a studied phenomenon. In this process, they can also learn about some previously unknown aspects and, as a consequence, start asking later interviewees about that aspects. E.g., as we realized the importance of delegation patterns and responsibility diffusion in some cases of non-updating behavior, we decided to ask more detailed questions about organizational structures and co-operation patterns in the second round of the data set 1 interviews (with web-shop owners). For extensive presentations of the GT methodology see the publications by Glaser and Strauss [20], Strauss and Corbin [37], as well as by Charmaz [9].

Triangulation: Triangulation is a methodological procedure developed mainly within the qualitative behavioral and social research. It allows looking at a studied phenomenon from various angles by combining different analytical methods, different data sets, different theoretical frames or/and different researcher perspectives in the process of conceptualization. In our present study, we specifically used a 'within-method data triangulation' according to Norman Denzin's triangulation typology [12]. This means that we used two different data sets generated and analyzed with the same methods: We conducted semi-structured interviews with members of two different groups (website owners and website professionals), and we analyzed these datasets in accordance with the GT methodology. A handbook chapter by Flick [17] offers an extensive introduction to the concept of triangulation in qualitative research.

B. Interview guide - website owners

Introduction: The researcher provides a brief summary of the study's purpose and introduces the interview (without explicitly mentioning the outdatedness of the participant's website). Then the participant will be informed again that the interview will be recorded and the recorded data will only be used for the purposes of the study.

- I would like to point out again that audio recordings will be taken during the interview. You can be assured that the data will only be used for the scientific purposes of this study and that the handling of your data will be GDPR compliant. Is this OK for you?

Semi-structured interview: The researcher now starts to ask open questions:

- We approached you because you are the owner of the website (xxx). So, I would like to start by asking you some general questions about your website.
- What does the website mean to you? What is its importance to you?
- Has the importance of your website changed since its creation?
- How long has your website existed?
- Did you create the website yourself?
- Do you regularly maintain the website yourself?
- Do you have someone you can turn to for technical support?
- If yes: How did this cooperation arise?
- If yes: Is there a formal agreement (maybe even a contract) that regulates the responsibilities?
- What do you do to secure your website against security risks?
- Have you had specific experiences with cyber attacks on your website?
- Have you ever thought about the consequences of not having an up-to-date version of Wordpress on your Website?
- What reasons have prevented you from updating to the latest version so far?
- What concerns do you have when you think about carrying out the update?

C. Interview guide - Web Developer

Introduction: The researcher starts the interview with questions about the websites the participant has created so far.

- What kind of websites have been created?

- How long have these websites been maintained?
- What was the experience of maintaining the websites?
- Were the websites maintained alone?
- How much time was invested in maintaining the website(s)?
- Which content management systems were used?
- How satisfied were you with the content management system used?

Updates for content management systems The researcher now asks specific questions on how to deal with updates in content management systems.

- Do website operators know what happens to their website / CMS when an update is made?
- What motivation do CMS providers have to issue updates?
- Are new updates installed regularly? Why or why not? Can you tell us more about this or give an example?
- How long do website operators wait until they carry out an update and why?
- How long do you wait before you update and why?
- What do you think could be improved in the update process?

D. Interview guide - Hosting provider

Introduction: At the beginning of the interview, the researcher first asks for information about the company and its philosophy. This is followed by questions about experience in hosting content management system-based, especially Wordpress-based, websites.

Key questions: After the more general questions at the beginning, the researcher goes more into details about the study topic:

- What challenges does hosting content management systems pose for the hoster? How are they dealt with? What communications strategies are used?
- Are outdated versions of content management systems a problem? If so, how does this manifest itself?
- Do you have an overview of compromised websites? How do you obtain this?
- With which issues / problems do customers approach you? How do you solve these problems?
- What do you think needs to be improved in the update process?
- What would help you?

E. Code Book Data Set 1

1) Value of the website
   - 1.1 Function / Use
     - 1.1.1 Customer acquisition
     - 1.1.2 Representation / Infos on the web
     - 1.1.3 Private use
     - 1.1.4 Sales tool
     - 1.1.5 Internally-directed benefits
     - 1.1.6 Financial benefit
   - 1.2 Future Plans
     - 1.2.1 Page rebuild
     - 1.2.2 Interview as motivation for updates
     - 1.2.3 Is support sought / aspired
2) Delegation
   - 2.1 Creation
     - 2.1.1 Self made
     - 2.1.2 External creation
   - 2.2 Content
     - 2.2.1 Responsibility maintenance respondent
     - 2.2.2 Responsibility maintenance external
   - 2.3 Updates
     - 2.3.1 External person named
     - 2.3.1 Dimensions of delegation
       - 2.3.1.1 Delegation pattern
       - 2.3.1.2 Formalization degree
       - 2.3.1.3 Coverage of delegation
       - 2.3.1.4 Communication pattern
   - 2.4 Problems of delegation
     - 2.4.1 Responsibility diffusion
     - 2.4.2 Disabling
     - 2.4.3 Inhibition to reach out
3) Threat and risk awareness
   - 3.1 No target
   - 3.2 Alternative security measures
4) Perceived risks of updates
   - 4.1 Impairment of functionality / design
   - 4.2 No concerns
5) Technical competence, understanding and skills
   - 5.1 Lack of understanding / know-how
   - 5.2 Technical support
     - 5.2.1 No technical support available
     - 5.2.2 Technical support available
     - 5.2.3 Support not necessary
   - 5.3 Updates no longer feasible / complicated

F. Code Book Data Set 2

1) Threat and risk awareness
   - 1.1 Risk awareness
   - 1.2 It will be alright
   - 1.3 Functionality over safety
   - 1.4 No attack surface
2) Responsibility diffusion
   - 2.1 Desire to hand over technical / security responsibility
   - 2.2 Sense of responsibility / competence
3) Technical competence, understanding and skills
   - 3.1 Technical know-how
   - 3.2 Technical maintenance as an ongoing process
   - 3.3 Curiosity