Exploring Transparent Communication for Organisational Cyber-Resilience to Sophisticated Phishing Attacks

Journal:	*Information and Computer Security*
Manuscript ID	ICS-01-2025-0024.R1
Manuscript Type:	Original Article
Keywords:	Lateral Phishing, Cybersecurity Practitioners, Incident Reporting, Spear Phishing, Transparent Communication

Exploring Transparent Communication for Organisational Cyber-Resilience to Sophisticated Phishing Attacks.

First Author's Name, Initials, and Last name*

First author's affiliation, an Institution with a very long name, xxxx@gmail.com

Second Author's Name, Initials, and Last Name

Second author's affiliation, possibly the same institution, xxxx@gmail.com

Third Author's Name, Initials, and Last Name

Third author's affiliation, possibly the same institution, xxxx@gmail.com

Sophisticated phishing attacks like lateral phishing have recently grown in complexity, posing a formidable challenge to conventional security measures. These attacks have evolved to become more advanced, making it difficult for users and security systems to detect and prevent them. We employed a qualitative research design to investigate the experiences of cybersecurity practitioners in countering these advanced phishing attacks by conducting semi-structured interviews with 13 practitioners (8 from the UK and 5 from India). The insights from cybersecurity practitioners highlight significant limitations and hesitations in sharing information about phishing incidents to the targeted employees. We found that the phishing threats intercepted before the employee interaction are typically not disclosed to the employee by the security practitioners. Practitioners face challenges in sharing information about phishing attempts and incidents due to privacy concerns, ongoing investigations, and potential reputational damage. We discuss the importance of transparent communication, especially in the context of sophisticated attacks.

1. INTRODUCTION

Sophisticated phishing attacks have become a growing concern in recent years as threat actors evolve to bypass traditional security measures. For instance, statistics show that sophisticated phishing attacks surged by 58.2% in 2023 compared to the previous year, with the average organisation receiving roughly five spear phishing emails per day – translating to over 1,700 attempts annually (Barracuda Networks, 2023; Desai Deepen and Hegde Rohit, 2024). Unlike bulk phishing, where a wide net is cast in hopes of compromising a few users with minimal effort, these targeted attacks leverage tailored social engineering techniques (Allodi *et al.*, 2020; Burns *et al.*, 2019). This includes not only spear phishing and Business Email Compromise (Cluley, 2023) but also the more insidious lateral phishing—attacks that move within an organization and exploit internal trust networks(Ho *et al.*, 2019).

Given the increasing sophistication and frequency of these attacks, cybersecurity practitioners are often compelled to lean on everyday employees to identify and report suspicious activity (Chitare *et al.*, 2023). However, this reliance is problematic because empirical evidence consistently demonstrates that employees generally possess poor mental models regarding phishing (Wash, 2010, 2020; Wash and Cooper, 2018), and their ability to recognise and report such threats is further hindered by suboptimal training retention and varying levels of awareness (Canova *et al.*, 2015; Ho *et al.*, 2017; Jenkins *et al.*, 2025). Interviews with security practitioners reveal an additional layer of complexity. Not only do practitioners acknowledge a strong dependence on employees for incident reporting (Chitare *et al.*, 2023), but they also face internal challenges in learning from such incidents due to fear of litigation if these are made public (Patterson *et*

* Place the footnote text for the author (if applicable) here.

al., 2023). This reticence is compounded by a failure to close the feedback loop with employees, who remain uninformed about mitigated threats and thus underprepared for future incidents.

The aim of this paper is to understand the barriers that security practitioners face when sharing information internally about sophisticated phishing attacks. Specifically, we ask: How do security practitioners share information about sophisticated phishing attacks within their organisations? In doing so, we explore opportunities for improving communication and user training for empowering employees while enhancing overall cybersecurity resilience.

2. LITERATURE REVIEW

2.1 Lateral Phishing Attacks

Research carried out by professionals (Ho *et al.*, 2019; Steve, 2017) and academics (Burström *et al.*, 2019; Egele *et al.*, 2017; Onaolapo *et al.*, 2016) has highlighted the increasing prevalence of lateral phishing attacks within the cybersecurity landscape. Lateral phishing represents a novel category of sophisticated phishing attacks, which primarily infiltrate a diverse range of organisations from within. This form of sophisticated attack is notably effective due to its exploitation of the inherent trust associated with internal email addresses, and benefiting from human recipients and conventional email security systems (Sutter *et al.*, 2022). Within the context of a lateral phishing attack, a targeted organisation's network node is compromised, enabling attackers to gain entry to the organisational network. Once infiltrated, these bad actors can get access to sensitive and valuable data, including but not limited to high-level employee credentials, financial records, intellectual property, and more (Bhadane and Mane, 2019). Lateral phishing attacks are highly dangerous due to their potential impact. The consequences of a successful lateral phishing attack can be severe, ranging from financial losses to reputational damage for individuals and organisations (Fang *et al.*, 2019). Furthermore, lateral phishing attacks can serve as a steppingstone for further intrusions or data breaches, as attackers gain a foothold within the target's network (Abbas *et al.*, 2021).

2.2 Security Practitioner Responses to Incidents

Cybersecurity practitioners play a crucial role in dealing with sophisticated phishing attacks. As bad actors continuously evolve their tactics to counter the solutions suggested by security practitioners, it is indeed essential to have practitioners who can stay updated with the latest trends and develop effective countermeasures (Do *et al.*, 2022). Previous work by Chitare et al (Chitare *et al.*, 2023) has shown that security practitioners prominently rely on the employees for the identification of sophisticated phishing attacks which may go unnoticed unless reported by the users. The work further states that employees are crucial in spotting and reporting compromised accounts and lateral attacks. Therefore, practitioners encouraged employees to report any suspected problems, favouring caution over excessive confidence. Other work by Patterson et al (Patterson *et al.*, 2023) highlights that practitioners also rely on the users for the incident response and improving overall cybersecurity posture. The work underscores that many practitioners can learn important lessons through users' experiences about security incidents. For instance, this work by Patterson et al. further reports that practitioners do not explicitly access the effectiveness of security practices. And practitioners in this study raised concerns regarding their organisations' fear of litigation or regulatory repercussions, which hindered their readiness to share incident information with other organisations. Although some participants shared sanitised lessons with regulators, exceeding legal requirements to benefit others in the industry, this practice was not common. Participants acknowledged the need for a mechanism that would enable organisations to share incident lessons without facing adverse consequences for doing so.

2.3 Employee Training

Of course, employees can only report suspected instances of phishing attacks if they have the appropriate knowledge and training to do so. Cybersecurity training programmes are designed to enhance employees' ability to detect and report phishing attempts (Ho *et al.*, 2017) through increased awareness of phishing tactics, and promote vigilance among users (Canova *et al.*, 2015). However, the effectiveness of such training is not always guaranteed, and organisations encounter several difficulties in achieving optimal results (Ho *et al.*, 2019).

One key challenge is ensuring long-term retention of training material. Previous work indicates that awareness and vigilance can decline over time, necessitating regular reminders and refresher training (Canova *et al.*, 2015). The content and delivery methods of training also

play a crucial role – interactive and engaging approaches tend to be more effective than passive methods (Briddick *et al.*, 2024; Canova *et al.*, 2015). Furthermore, the complexity of phishing emails and individual user characteristics can influence the success of training interventions (Ho et al., 2024).

Beyond training, organisations must establish robust incident response processes to handle phishing events effectively. These processes should encompass clear communication channels and coordinated efforts across different departments (Althobaiti *et al.*, 2021). User reporting of suspicious emails is a critical component of incident response, enabling timely identification and mitigation of potential threats (Burda *et al.*, 2020). However, several factors can deter users from reporting phishing emails, including a lack of awareness, uncertainty about the legitimacy of the email, and perceived time constraints (Kwak *et al.*, 2020).

Employees' experiences with phishing training can vary significantly. Some may find the training beneficial and empowering (Chen *et al.*, 2024), leading to increased confidence in their ability to detect and report phishing attempts. Others may perceive the training as burdensome or ineffective (Chen *et al.*, 2024), particularly if they lack a clear understanding of its purpose or if the training materials are not relevant to their specific roles. Moreover, fear of blame or a lack of confidence in the incident response process can discourage users from reporting phishing incidents (Althobaiti *et al.*, 2021).

Therefore, a comprehensive approach to addressing phishing requires not only effective user training but also a supportive organisational culture that encourages reporting and provides clear guidance on incident response procedures (Althobaiti *et al.*, 2021). Understanding the motivations and deterrents for employee participation in phishing interventions is crucial for designing and implementing successful programs (Chen *et al.*, 2024) and recent work has begun to explore novel ways of eliciting these motivations (e.g., through anonymous discussion systems (Jenkins *et al.*, 2025) and interactive ranking tasks (Nicholson *et al.*, 2017). Additionally, analysing user justifications for reporting (or not reporting) phishing emails can provide valuable insights into their perceptions and decision-making processes (Pilavakis *et al.*, 2023). By addressing these challenges and incorporating user feedback, organisations can enhance their ability to mitigate the risks associated with phishing attacks.

3. METHODOLOGY

3.1 Research Design

A qualitative research design was chosen for this study to explore the experiences, perceptions, and practices of cybersecurity practitioners in dealing with sophisticated phishing attacks. This approach allowed for an in-depth exploration and understanding of the participants' perspectives and provided rich, contextualised data (Nifakos *et al.*, 2021).

Semi-structured interviews were conducted with 13 cybersecurity practitioners as the primary method of data collection. Out of the 13 participants, 8 were from the UK and 5 were from India, ensuring a diverse range of perspectives (see Table I). This approach allowed for flexibility in exploring the participants' responses in detail while maintaining a consistent focus on the research questions (Nifakos *et al.*, 2021). Open-ended questions were used to elicit participants' views on incident response strategies, challenges faced, best practices, and lessons learned (see Appendix I). The questions were based on existing academic literature, focusing on themes such as incident response strategies, incident handling processes, resource allocation, collaboration with stakeholders, challenges faced, and lessons learned (Alothman *et al.*, 2022; Kara *et al.*, 2022; Rantos *et al.*, 2020). The interviews were conducted online for the convenience of participants, and each interview lasted approximately 45-60 minutes. The interviews were audio-recorded to ensure accuracy during analysis. This study received approval from our institution's Research Ethics Committee.

3.2 Participant Selection

Security practitioners were defined as individuals who were employed full-time in a position where they were primarily responsible for the security of their organisation and had at least 12 months of experience in similar positions. Participants were recruited through professional networks, cybersecurity conferences, and industry associations. Invitations were sent via email, providing information about the study's objectives, voluntary participation, and confidentiality assurances (Nifakos *et al.*, 2021). This recruitment strategy ensured that participants had relevant experience and practice in dealing with sophisticated phishing attacks in their organisations.

Table I. Demographics of the participants

Number	Country	Designation	Experience in years	Organisation Size
Practitioner 1	UK	Cybersecurity Engineer	10	SME
Practitioner 2	Australia	Chief Information Security Officer	13	Large
Practitioner 3	UK	Security Researcher (recently expatriated from the UK)	3.5	Large
Practitioner 4	India	Security Delivery Associate Manager	13	Large
Practitioner 5	India	Senior Cybersecurity Analyst	8	SME
Practitioner 6	India	Senior Cybersecurity Analyst	7	Large
Practitioner 7	India	Incident responder and analyst	5	Large
Practitioner 8	UK	Information & Cyber Security Manager	10	SME
Practitioner 9	India	Information security officer	8	Large
Practitioner 10	UK	Head of the security team and Principal security engineer	17	Large
Practitioner 11	UK	Security Consultant	5	SME
Practitioner 12	UK	Security Auditor	15	SME
Practitioner 13	UK	Director of Cybersecurity	15	Large

3.3 Data Analysis

Reflexive thematic analysis, as described by Braun and Clarke (Braun and Clarke, 2012), was employed to analyse the interview data for obtaining a deep understanding of practitioner perspectives on sophisticated phishing attacks. The initial coding was conducted independently by the first author (who also conducted the interviews), and consensus was reached on the identified themes through discussion with the whole team at various touch points. By using an inductive approach, codes were identified that were solely reflective of the content of the data free from any pre-conceived theory or conceptual framework.

The transcripts were generated during the interviews on MS Teams using the live transcription (an option in MS Teams) alongside the interview in real time. In the live transcript the 'English (UK)' language option was selected for participants from UK and 'English (India)' option was selected for participants from India. These transcripts were read along with the video two to three times to make the required corrections to ensure they were verbatim (Phase 1: Familiarisation with data). While familiarity was gained with the depth and breadth of data during this step, notes were also taken in MS Word about the initial trends in the data and potentially interesting passages in the transcripts. These notes were used to get the initial data items that were useful in addressing the research question (Phase 2: Generating initial code). Once the coding process confirmed that no new relevant codes were identified, following an iterative process where all transcripts were coded, and the initial transcripts were revisited for a second pass to ensure saturation, the data items were transferred to spreadsheet in MS Excel where the preliminary iteration of coding was done. Subsequent iterations of coding were also done and documented in this spreadsheet (Byrne, 2022). Once the lead author completed the first pass at coding, these were reviewed by the third author and any disagreements were discussed until consensus was reached. The first author proceeded to edit codes accordingly before these were reviewed by the second and third authors. After finalising the codes from all the participants, the coded data was reviewed to form themes according to their shared meaning (Phase 3: Generating themes). After the first pass at the analysis by the first author, the whole research team looked through the themes, the codes, and a selection of the participant quotes. The same process was followed after a second iteration of the theming processes. Once all members of the research team were confident that the themes represented the experiences of participants, they were finalised by the first author (Phase 4: Reviewing potential themes). During the discussion with the team, some themes had to be split into subthemes and later on all the themes and subthemes were grouped together to create a hierarchy of themes including the sub themes. Themes were named either highlighting the important aspects or using short extracts

in the data items (Phase 5: Defining and naming Themes). Finally, the findings from the themes were reported to facilitate further discussions (Phase 6: Producing the report). For an abridged version of our final codebook please see Appendix II.

4. RESULTS

In this section we present two themes that encompass the limitations of practitioners in sharing information about phishing attempts (4.1) and about phishing incidents (4.2) which in turn limit the learning of the organisation and prevent transparent communication.

4.1 Phishing attempts are not reported to users if they are resolved before the users see it

A common strategy observed among cyber security practitioners involves not reporting phishing attempts to users if they are resolved before user detection. This approach is underscored by the belief that early interception of such threats ensures a 0% chance of user interaction, as articulated by (UK) Practitioner 1:

"If we can remove that e-mail before they (users) ever find out, we will. We don't if they've opened the e-mail, then we tell the user to reset their password and possibly do that. But if we can detect fully that they haven't opened it, we don't contact the user. Well, because we don't. If we can get to it before an end user sees it, there's 0% chance that they're gonna click it. So that there's a 0% chance that they're gonna interact with it ***if we can get to it before they can. So, we want to get rid of it as soon as possible as well, just to make sure that we are keeping the organisation as secure as possible****… because if there is e-mail sitting about in inboxes, that could lead to potential compromise. It's even if it is a genuine mistake, they don't click it maliciously. They can still click it by accident or enter credentials.*

By removing phishing emails before users can see them, the risk of accidental clicks or credential entry is entirely mitigated. This pre-emptive measure is critical in maintaining the organisation's security posture, as even unintentional user actions can lead to severe vulnerabilities. Of course, what this means is that then users are not exposed to potential phishing attacks, which then cannot be used as a frame of reference for detecting future attacks and also obscure the efforts that practitioners exert in maintaining organisational security.

(India) *Practitioner 6 –"Even if we observe a sophisticated phishing attack on a particular user* ***we don't inform this particular user personally, rather we send a generalised email to the whole organisation*** *saying that such kind of attack or incident was observed. Like there was an instance where a phishing email was sent from a single sender (compromised account) to multiple recipients. So, in that case whoever the recipients were, we sent out the advisory email to them. We send out as advisory email that you have received an email from so and so user during so and so time with the subject line so and so and you just ignore that email and do not respond to it. And if you have responded just let us know."*

In cases where sophisticated phishing attacks have been identified following their delivery to a user's inbox, Practitioner 6 indicates that individual notifications to affected users are not standard practice. Instead, a generalised email is sent to the entire organisation, notifying them of the incident without singling out specific users. This approach maintains a broader awareness of phishing threats while avoiding potential panic or undue concern among individual users. It also suggests a strategy of disseminating information that reinforces general vigilance rather than focusing on isolated incidents. Additionally, in instances where phishing emails are sent from compromised accounts to multiple recipients, Practitioner 6 describes sending advisory emails to the affected recipients. These advisories include specific details about the phishing attempt, such as the sender, time, and subject line, instructing recipients to ignore the email and report if they have engaged with it, but do not use these as training opportunities (e.g., by explaining *why* it is a sophisticated phishing message).

*(UK) Practitioner 10 – "We don't specifically call it out, I mean, it's all the usual stuff of, you know, check the content, check does it have an external banner on it? …****we don't specifically talk about internal lateral phishing, certainly not to our end users.*** *We talk about it within the security space, and which is why we have always protections in place, but we don't talk about it to our own users."* Practitioner 10's comments further illustrate the internal handling of phishing attempts, noting that discussions about internal lateral phishing are confined within the security team and not extended to end users. This internal focus ensures that security measures are continually evaluated and updated without causing unnecessary alarm among users. The practitioners' collective approach underscores a strategic balance between pre-emptive threat removal and selective communication, aiming to maintain security without overwhelming users with frequent alerts.

4.2 There are limitations to sharing information about phishing incidents

The insights gathered from interviews with cybersecurity practitioners reveal notable limitations and hesitations in sharing information about phishing incidents internally with end users, and externally with other parties. These limitations primarily stem from concerns over privacy regulations, the impact on organisational reputation, and the complexities of ongoing investigations.

(UK)Practitioner 10 – "So, we try, and I'll be honest with you, ***our approach is how little can we have our users think and do so they don't have to worry about it****. What controls can we put around them so that it just isn't a problem? And that's the approach that we tend to take. We are we have too many people that we can't train everyone to the right level. We have to assume that we have people who will click the wrong thing that and enter their details…….It could be some of* ***it I feel because of the risk of GDPR privacy on that and you know****, for example, there have been times sometime if it's in the middle of an investigation. Obviously, you don't wanna tell the wrong people the facts actively. So yeah, I think sometimes there's a limit to what we're doing, what we're told until a certain time."*

One of the prominent reasons for the reluctance to share details about phishing incidents is the risk associated with data protection legislation, which supports previous findings from Patterson et al., (2023). However, this was exclusive to UK practitioners, who mentioned the Data Protection Act 2018 and its predecessor the General Data Protection Regulation and exclusive to sharing externally. For example, Practitioner 10 explicitly mentions the constraints imposed by GDPR, which necessitate cautious handling of personal data and can impede transparent communication during incident investigations. This regulation requires organisations to protect individuals' privacy and restricts the dissemination of information that might lead to breaches of personal data. Consequently, cybersecurity practitioners are often hesitant to share detailed information about incidents, fearing potential legal repercussions. Additionally, the need to safeguard ongoing investigations contributes to this hesitancy. Practitioner 10 notes that during active investigations, divulging too much information prematurely can compromise the integrity of the investigation. Sharing specifics about the phishing incident might inadvertently tip off malicious actors or lead to the spread of misinformation, complicating the resolution process. This need for confidentiality often limits the amount of information that can be shared externally until the investigation reaches a conclusive stage. However, once investigations are concluded, more information could be shared with employees to create a grounded learning experience – something that no practitioners reported doing.

On the other hand, security practitioners based in India were hesitant to share details of phishing incidents due to potential repercussions to company's reputation.

(India) Practitioner 7- "The user did click the links and he was not aware of what was happening at the backend. This account was used to send around 150 emails to the (company name) in (country name). Then the security team of that organisation got in touch with us stating that they had received such emails recently. And provide us with the sender ID and other details of the malicious files used in the email. After this, we got in touch with the user for more information and simultaneously started doing other analysis and sanitisation processes. We did reset the account and applied relevant policies. We did acknowledge that company that necessary steps are taken but ***we did not mention the account compromise instead we made up a fake story with technical issues as it might have impacted the brand and image our organisation".***

Loyalty to the organisation appeared to play a role in obfuscating phishing incidents amongst Indian participants. For example, Practitioner 7 illustrates this by describing an incident where a compromised account was used to send phishing emails. To protect the organisation's reputation, the practitioner chose not to disclose the account compromise to the affected organisation, instead attributing to technical problems. This approach underscores the concern that admitting security breaches could tarnish the organisation's public image and erode trust among clients and partners, despite legislation requiring them to do so.

It is not surprising to see different motivations reported by practitioners in India and the UK. Research has shown that individuals from individualistic cultures tend to emphasise personal traits and behaviours (Sedikides *et al.*, 2003), while those from collectivistic cultures are more likely to prioritise group memberships and collective identities (Akter *et al.*, 2022). Cultural diversity plays a significant role in shaping attitudes towards cybersecurity awareness and education. For instance, individuals from collectivist cultures may have different perceptions of cybersecurity threats compared to those from individualistic cultures (Akter *et al.*, 2022). Furthermore, the development of a cybersecurity culture and an understanding of cybersecurity threats are particularly important in today's culturally diverse

society (Piščikienė *et al.*, 2021). Then, we see how practitioners in India value organisational loyalty and thus limit details of phishing incidents in order to protect the organisation, while UK practitioners are guided by data protection legislation. Of course, given the qualitative approach to this study it is not possible to say that all UK or India practitioners are motivated by these principles, but it is interesting to observe how different motivations lead to a similar outcome that could negatively affect the transparent communication within organisations and impact learning opportunities for both employees and practitioners.

Additionally, the interactions between different organisational roles further complicate the information-sharing landscape.

(UK) Practitioner 11- "If this happens with the clients, we are taking care of they have their own security teams. They would ring us and ask us about it. We'd consult them with the best course of action in terms of things like with cyber essentials, a lot of them are Cyber Essentials……And because the clients a lot of them are big, like for example, (Name) University is one of our clients and they'll have their internal policies and how they deal with them. ***We don't tend to get involved in internals being a consultancy company.*** *If they need advice will give advice, but* ***we wouldn't be the ones that pick it up first****."* Practitioners like Practitioner 11, who work for consultancy companies, highlight the intricate dynamics of managing client relationships. Clients often have their internal security policies and teams, and consultants provide advice rather than direct intervention. This separation can create a disconnect in how information is shared and managed, with consultants being cautious about overstepping boundaries or providing unsolicited details.

Finally, practitioners from both countries emphasised the importance of involving line managers in incident communication:
Practitioner 8- "I'll go and contact often their line manager to confirm that that person is the person we think it is."
(India) Practitioner 5- "We communicate with the manager and inform them about the incident. We always keep the manager in the loop for such a type of communication. ***The manager further communicates with the employee****."*

This hierarchical approach ensures that information is filtered and managed appropriately within the organisation but may also introduce delays and barriers to immediate transparency. Managers act as intermediaries, which can sometimes lead to diluted or altered communication about the incident, further limiting the breadth and accuracy of information shared.

5. DISCUSSIONS

The insights from cybersecurity practitioners highlight significant limitations and hesitations in sharing information about phishing attempts and incidents both internally and externally. Concerns over data protection legislation compliance, organisational reputation, and the complexities of ongoing investigations are primary factors for not sharing details of phishing incidents more widely. Practitioners also reported keeping line managers in the loop during incident communications, which can introduce delays and barriers to transparency. Phishing attempts are often not reported to users if resolved before detection to ensure zero user interaction which is seen as paramount for maintaining the overall security of the organisation. Instead, practitioners usually follow a strategy of sending generalised advisory emails rather than individual notifications for sophisticated attacks, promoting overall awareness without causing undue concern. Internal discussions on phishing attempts are kept within the security team to avoid alarming end users, although this is potentially a missed opportunity to improve the training provision for employees where specific context and examples can make these incidents memorable and help detection in the future (Briddick *et al.*, 2024) as well as learn from incidents (Patterson *et al.*, 2023).

5.1 Is transparent internal communication possible?

Transparent communication, i.e., being honest with end users about mitigated sophisticated attacks, can help build trust and understanding between security practitioners and other employees, leading to more effective collaboration in preventing and responding to attacks (Rumble and Irani, 2016). One of the key benefits of transparent communication is that it enables employees to have a better understanding of the security risks and challenges faced by the organisation. This understanding can help employees make informed decisions about security investments and prioritise security measures (Werlinger *et al.*, 2009). Transparent communication also allows employees to provide valuable input and feedback on security practices, which can help identify vulnerabilities and improve security measures (Werlinger *et al.*, 2009). Furthermore, transparent communication can enhance the effectiveness of incident response efforts. In the interviews with the security practitioners, we observed that there are certain limitations to sharing information about the cyber-attacks experienced in their organisations, particularly about the sophisticated attacks. This may be for a number of reasons.

In section 3.2 Practitioner 10 was concerned about the potential violation of privacy regulations, such as the General Data Protection Regulation (GDPR), which could occur when sharing information about phishing incidents. This concern is supported by (Lee *et al.*,

2023), which discusses the role of privacy concerns in phishing victimisation. The authors suggest that privacy concerns can influence individuals' attitudes towards sharing personal information online, which in turn can affect their susceptibility to phishing attacks. The practitioner states that there are times when it is not appropriate to share information about phishing incidents, especially when an investigation is still in progress. This is because sharing such information could potentially compromise the investigation or alert the wrong people. This concern aligns with other existing work (Gordon *et al.*, 2019), which discusses the common threat of phishing attacks against hospital employees. The authors emphasise the importance of cybersecurity risk management in healthcare systems, including the need to protect ongoing investigations.

In the real example provided by Practitioner 7 in section 3.2 we observe a fake story that was fabricated by the practitioner. By acknowledging the account compromise, the practitioner's organisation would have had to admit a security breach, which could lead to a loss of trust from clients and stakeholders. Hence, practitioners may resort to downplaying or masking the true nature of incidents to maintain a positive perception of their organisation. This aligns with the findings of (Gallagher *et al.*, 2003), which discusses the attitudes of physicians towards disclosing medical errors. The study highlights that practitioners may hesitate to disclose errors due to concerns about the impact on their professional reputation and the reputation of their organisation. However, the practitioner's decision to fabricate a fake story instead of disclosing the account compromise may have been driven by a desire to protect the user's privacy and prevent further harm. This aligns with the findings of (Lin *et al.*, 2016), that individuals may be reluctant to disclose sensitive information due to fears of stigma, discrimination, and negative consequences (Lin *et al.*, 2016). Furthermore, the fear of reputational damage and financial loss can also contribute to the hesitancy to share phishing incidents. Phishing attacks are a major cyber threat that can cause significant financial and reputational damage to organisations (Gamisch and Pöhn, 2023). The disclosure of phishing incidents may expose vulnerabilities in an organisation's security measures and could potentially harm its reputation and financial standing.

In another instance, as mentioned by Practitioner 11 in section 3.2 the practitioners who are working as a consultant or working for a consultancy prefer to advise the clients in the event of sophisticated attacks rather than direct intervention. Most importantly, the practitioner further admits that in such events *'we wouldn't be the ones that pick it up first'* showing that there are certain boundaries and limitations within which the practitioners have to work. Practitioners also highlighted that they would first inform the line managers in the event of a security incident. This hierarchical communication may be a part of the communication protocol, else the practitioners might not have other alternatives to inform the affected employee. In hierarchical structures, the transmission of messages from top-level management to lower-level employees and vice versa can be challenging, impacting the timeliness and accuracy of communication resulting in misunderstandings, decreased efficiency, and reduced overall organisational performance (Zaira *et al.*, 2022). Studies have shown that hierarchical communication can limit interactions between individuals within teams and departments, as well as with external stakeholders, impeding knowledge sharing and collaboration (Darmawan *et al.*, 2023).

It is understandable that security practitioners are hesitant to share information about ongoing incidents. Yet, participants did not present a reason why sharing details *internally* once the incident had been resolved would be a problem, other than worrying users. However, by not openly discussing these incidents, organisations can be missing out on learning opportunities for both practitioners (Patterson *et al.*, 2024) (learning more about how end users respond to concrete phishing attacks, their reflections on materials, etc.) and employees (exposure to less obvious phishing messages that can provide a template for future detection).

5.2 Prioritising prevention over response

Based on the insights from the practitioners it is clear that they prefer to prevent an attack rather than have to respond to it. Being overly cautious and removing all phishing messages, and then potentially not even showing them ever to targeted employees, it creates a situation where valuable training materials are not being used. The statements by Practitioner 1 in section 3.1 signifies practitioner's perspective that the swift elimination of threats not only prevents immediate risk but also maintains a secure environment by reducing the potential for compromise. This method may reflect a proactive stance in cybersecurity management, prioritising prevention over response. But it may also lead to a potential gap in the effective and swift communication needed in the effect of sophisticated attacks between security practitioners and the employees. We know that practitioners heavily rely on employee reports to start dealing with sophisticated attacks which otherwise may go unnoticed (Chitare *et al.*, 2023). So, if an employee is targeted with a phishing email that is intercepted by the

security teams and taken care of without informing the employee, there are chances that the employee might be targeted again and this time phishing email may land successfully in the employees' inbox. Thus, the employee remains vulnerable to the potential future threat. On the other hand, if the practitioners intercept and take care of the phishing message, the targeted employee can be briefed with a personalised message giving details of the attacks and security guidelines in such a scenario and could even be used more widely within the team or the whole organisation as case study material.

In the statement from Practitioner 6 in section 3.1 we observed that the approach of sending a generalised email to the whole organisation is a common practice in cybersecurity. The purpose of this approach is to raise awareness among all users about the phishing attack or incident that was observed. By informing the entire organisation, it helps to ensure that all users are vigilant and cautious when it comes to potential phishing attacks (Lallie *et al.*, 2021). The reason behind not informing the specific user individually is not mentioned in the response. However, it can be inferred that this approach is taken to avoid causing panic or singling out the targeted user. By sending a generalised email, the organisation can maintain a sense of unity and collective responsibility in addressing cybersecurity threats. It is important to note that this approach may have its limitations. While it helps to raise awareness among all users, it may not provide specific guidance or instructions to the targeted user on how to respond to the phishing attack. In some cases, it may be necessary to provide individualised support and guidance to the affected user to mitigate the impact of the attack (Lallie *et al.*, 2021). It may be useful to personally inform the targeted user as this may make the user more vigilant in encountering and identifying potential threats in similar scenarios in the future. Further, Practitioner 6 makes it clear that when a sophisticated attack like lateral phishing, which typically affects multiple employees, is identified an advisory email was sent to the affected employes suggesting to '*ignore that email and do not respond to it'*. This targeted communication may balance between informing users of specific threats they may have encountered and maintaining overall organisational security awareness, but this again leaves the employees vulnerable to future attacks and they asked to ignore it, rather the advisory mail might have brief about necessary actions in such event.

5.3 Limiations and Future work

The insights obtained from this work are not generalisable to all UK or Indian security practitioners. This work did not particularly focus on comparing the diverse participants to identify the differences in organisation size or cultural background but instead looked at the experiences of practitioners in this underexplored area of communications around sophisticated phishing attacks. Additionally, the use of convenience sampling means that security practitioners with similar and/or overlapping experiences may have been recruited, which means more work is needed to understand the range of experiences and behaviours with this user group. Future research could explore specific characteristics of employees/organisations at a larger scale. This would provide a more comprehensive understanding of the effectiveness of organisational defences against lateral phishing attacks across different contexts. Future work can focus on examining the impact of not informing the targeted users about mitigated phishing attacks on their ability to recognise and respond to future threats which could provide valuable insights for crafting more comprehensive training programmes.

6. CONCLUSION

In this paper we report on our initial exploration about limitations and hesitations of the security practitioners in sharing the information about sophisticated attacks with the targeted employee in the organisation. We did this through interviews with 13 security practitioners from the UK and India and detailed the complex dynamics of information sharing among security practitioners regarding sophisticated phishing attacks. Through interactive interviews with the security practitioners, we found that despite recognising the need for better employee training, practitioners often hesitate to disclose details about such incidents due to privacy regulations, organisational reputation concerns, and the intricacies of ongoing investigations even after incidents had been fully resolved. While pre-emptive measures to intercept phishing threats before users can engage with them are effective, they also limit users' exposure to potential phishing tactics, hindering their ability to learn and recognise such threats in the future.

REFEENCES

Abbas, S.G., Vaccari, I., Hussain, F., Zahid, S., Fayyaz, U.U., Shah, G.A., Bakhshi, T., *et al.* (2021), "Identifying and Mitigating Phishing Attack Threats in IoT Use Cases Using a Threat Modelling Approach", *Sensors*, Vol. 21 No. 14, p. 4816, doi: 10.3390/s21144816.

Akter, S., Uddin, M.R., Thomas Lee, W.J., Michael, K. and Hossain, M.A. (2022), "Reconceptualizing Cybersecurity Awareness Capability in the Data-Driven Digital Economy", *Annals of Operations Research*, doi: 10.1007/s10479-022-04844-8.

Allodi, L., Chotza, T., Panina, E. and Zannone, N. (2020), "The Need for New Antiphishing Measures against Spear-Phishing Attacks", *IEEE Security and Privacy*, Institute of Electrical and Electronics Engineers Inc., Vol. 18 No. 2, pp. 23–34, doi: 10.1109/MSEC.2019.2940952.

Alothman, B., Alhajraf, A., Alajmi, R., Al Farraj, R., Alshareef, N. and Khan, M. (2022), "Developing a Cyber Incident Exercises Model to Educate Security Teams", *Electronics 2022, Vol. 11, Page 1575*, Multidisciplinary Digital Publishing Institute, Vol. 11 No. 10, p. 1575, doi: 10.3390/ELECTRONICS11101575.

Althobaiti, K., Jenkins, A.D.G. and Vaniea, K. (2021), "A Case Study of Phishing Incident Response in an Educational Organization", *Proceedings of the ACM on Human-Computer Interaction*, ACM PUB27 New York, NY, USA , Vol. 5 No. CSCW2, pp. 1–32, doi: 10.1145/3476079.

Barracuda Networks. (2023), *Spear-Phishing Trends : Key Findings about the Impact of Attacks and the Challenges of Threat Detection and Response*.

Bhadane, A. and Mane, S.B. (2019), "Detecting lateral spear phishing attacks in organisations", *IET Information Security*, The Institution of Engineering and Technology, Vol. 13 No. 2, pp. 133–140, doi: 10.1049/IET-IFS.2018.5090.

Braun, V. and Clarke, V. (2012), "Thematic analysis.", *APA Handbook of Research Methods in Psychology, Vol 2: Research Designs: Quantitative, Qualitative, Neuropsychological, and Biological.*, American Psychological Association, Washington, doi: 10.1037/13620-004.

Briddick, C., Briggs, P. and Nicholson, J. (2024), "Using Breach and Attack Demonstrations to Explain Spear Phishing Attacks to Young Adults", pp. 65–80, doi: 10.1007/978-3-031-62918-1_5.

Burda, P., Chotza, T., Allodi, L. and Zannone, N. (2020), "Testing the effectiveness of tailored phishing techniques in industry and academia: A field experiment", *ACM International Conference Proceeding Series*, Association for Computing Machinery, doi: 10.1145/3407023.3409178.

Burns, A.J., Johnson, M.E. and Caputo, D.D. (2019), "Spear phishing in a barrel: Insights from a targeted phishing campaign", *Journal of Organizational Computing and Electronic Commerce*, Taylor and Francis Inc., Vol. 29 No. 1, pp. 24–39, doi: 10.1080/10919392.2019.1552745.

Burström, G., Swamy, A., Spliethoff, J.W., Reich, C.G., Babic, D., W. Hendriks, B.H., Skulason, H., *et al.* (2019), "Diffuse Reflectance Spectroscopy Accurately Identifies the Pre-Cortical Zone to Avoid Impending Pedicle Screw Breach in Spinal Fixation Surgery", *Biomedical Optics Express*, doi: 10.1364/boe.10.005905.

Byrne, D. (2022), "A worked example of Braun and Clarke's approach to reflexive thematic analysis", *Quality & Quantity*, Springer Science and Business Media B.V., Vol. 56 No. 3, pp. 1391–1412, doi: 10.1007/s11135-021-01182-y.

Canova, G., Volkamer, M., Bergmann, C., Borza, R., Reinheimer, B., Stockhardt, S. and Tenberg, R. (2015), "Learn to Spot Phishing URLs with the Android NoPhish App", *IFIP Advances in Information and Communication Technology*, Springer, Cham, Vol. 453, pp. 87–100, doi: 10.1007/978-3-319-18500-2_8.

Chen, X., Doublet, S., Sergeeva, A., Lenzini, G., Koenig, V. and Distler, V. (2024), "What Motivates and Discourages Employees in Phishing Interventions: An Exploration of Expectancy-Value Theory", *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, USENIX Association, Philadelphia, PA, pp. 487–506.

Chitare, N., Coventry, L. and Nicholson, J. (2023), "'It may take ages': Understanding Human-Centred Lateral Phishing Attack Detection in Organisations", *Proceedings of the 2023 European Symposium on Usable Security*, ACM, New York, NY, USA, pp. 344–355, doi: 10.1145/3617072.3617116.

Cluley. (2023), "US charges three men with six million dollar business email compromise plot", *Tripwire*, 20 April, available at: https://www.tripwire.com/state-of-security/us-charges-three-men-six-million-dollar-business-email-compromise-plot (accessed 15 March 2024).

Darmawan, S., Agusvina, N., Lusa, S. and Sensuse, D.I. (2023), "Knowledge Management Factors and Its Impact on Organizational Performance: A Systematic Literature Review", *JOIV : International Journal on Informatics Visualization*, Politeknik Negeri Padang, Vol. 7 No. 1, pp. 161–167, doi: 10.30630/JOIV.7.1.1644.

Desai Deepen and Hegde Rohit. (2024), "Phishing Attacks Rise 58% in the Year of AI: ThreatLabz 2024 Phishing Report | Zscaler", *Zscaler* , 23 April, available at: https://www.zscaler.com/blogs/security-research/phishing-attacks-rise-58-year-ai-threatlabz-2024-phishing-report (accessed 19 July 2024).

Do, N.Q., Selamat, A., Krejcar, O. and Fujita, H. (2022), "Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions", *Ieee Access*, doi: 10.1109/access.2022.3151903.

Egele, M., Stringhini, G., Kruegel, C. and Vigna, G. (2017), "Towards Detecting Compromised Accounts on Social Networks", *Ieee Transactions on Dependable and Secure Computing*, doi: 10.1109/tdsc.2015.2479616.

Fang, Y., Zhang, C., Huang, C., Liu, L. and Yang, Y. (2019), "Phishing Email Detection Using Improved RCNN Model With Multilevel Vectors and Attention Mechanism", *IEEE Access*, Institute of Electrical and Electronics Engineers Inc., Vol. 7, pp. 56329–56340, doi: 10.1109/ACCESS.2019.2913705.

Gallagher, T.H., Waterman, A.D., Ebers, A.G., Fraser, V.J. and Levinson, W. (2003), "Patients' and Physicians' Attitudes Regarding the Disclosure of Medical Errors", *JAMA*, Vol. 289 No. 8, p. 1001, doi: 10.1001/jama.289.8.1001.

Gamisch, L. and Pöhn, D. (2023), "A Study of Different Awareness Campaigns in a Company", *Proceedings of the 18th International Conference on Availability, Reliability and Security*, ACM, New York, NY, USA, pp. 1–8, doi: 10.1145/3600160.3605006.

Gordon, W.J., Wright, A., Glynn, R.J., Kadakia, J., Mazzone, C., Leinbach, E. and Landman, A. (2019), "Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system", *Journal of the American Medical Informatics Association*, Vol. 26 No. 6, pp. 547–552, doi: 10.1093/jamia/ocz005.

Ho, G., Gavish, L., Schweighauser, M., Networks, B., Paxson, V., Berkeley, U., Savage, S., *et al.* (2019), "Detecting and Characterizing Lateral Phishing at Scale", *28th USENIX Security Symposium*.

Ho, G., Sharma, A., Javed, M., Paxson, V. and Wagner, D. (2017), "Detecting Credential Spearphishing Attacks in Enterprise Settings", *26th USENIX Security Symposium*.

Jenkins, E., Abdulgalimov, D., Briggs, P., Olivier, P. and Nicholson, J. (2025), "Using Anonymous Discussion Platforms to Support Open Conversations about Cybersecurity in Organisations", *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, ACM, New York, NY, USA, pp. 1–14, doi: 10.1145/3706598.3713290.

Kara, S.;, Hizal, S.& and Zengin, A. (2022), "DESIGN AND IMPLEMENTATION OF A DEVS-BASED CYBER-ATTACK SIMULATOR FOR CYBER SECURITY", *Int j Simul Model*, Vol. 21, pp. 53–64, doi: 10.2507/IJSIMM21-1-587.

Kwak, Y., Lee, S., Damiano, A. and Vishwanath, A. (2020), "Why do users not report spear phishing emails?", *Telematics and Informatics*, Vol. 48, p. 101343, doi: 10.1016/j.tele.2020.101343.

Lallie, H.S., Shepherd, L.A., Nurse, J.R.C., Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X. (2021), "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks During the Pandemic", *Computers &Amp; Security*, doi: 10.1016/j.cose.2021.102248.

Lee, Y.Y., Gan, C.L. and Liew, T.W. (2023), "Thwarting Instant Messaging Phishing Attacks: The Role of Self-Efficacy and the Mediating Effect of Attitude towards Online Sharing of Personal Information", *International Journal of Environmental Research and Public Health*, Vol. 20 No. 4, p. 3514, doi: 10.3390/ijerph20043514.

Lin, X., Chi, P., Zhang, L., Zhang, Y., Fang, X., Qiao, S. and Li, X. (2016), "Disclosure of HIV Serostatus and Sexual Orientation Among HIV-Positive Men Who Have Sex with Men in China", *Community Mental Health Journal*, Springer New York LLC, Vol. 52 No. 4, pp. 457–465, doi: 10.1007/S10597-015-9879-Z/TABLES/2.

Nicholson, J., Coventry, L. and Briggs, P. (2017), "Introducing the Cybersurvival Task: Assessing and Addressing Staff Beliefs about Effective Cyber Protection", *USENIX Symposium on Usable Privacy and Security (SOUPS)*.

Nifakos, S., Chandramouli, K., Nikolaou, C.K., Papachristou, P., Koch, S., Panaousis, E. and Bonacina, S. (2021), "Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review", *Sensors*, Vol. 21 No. 15, p. 5119, doi: 10.3390/s21155119.

Onaolapo, J., Mariconti, E. and Stringhini, G. (2016), "What Happens After You Are Pwnd", *Proceedings of the 2016 Internet Measurement Conference*, ACM, New York, NY, USA, pp. 65–79, doi: 10.1145/2987443.2987475.

Patterson, C.M., Nurse, J.R. and Franqueira, V.N. (2024), "'I don't think we're there yet': The practices and challenges of organisational learning from cyber security incidents This document version Additional information Versions of research works 'I don't think we're there yet': The practices and challenges of organisational learning from cyber security incidents Keywords: Cyber security incidents Organisational learning Post-incident review Cyber resilience Learning practices Lessons learned Neo-institutional theory Isomorphic pressures", *Computers & Security*, Vol. 139, p. 103699, doi: 10.1016/j.cose.2023.103699.

Patterson, C.M., Nurse, J.R.C. and Franqueira, V.N.L. (2023), "Learning from cyber security incidents: A systematic review and future research agenda", *Computers & Security*, Vol. 132, p. 103309, doi: 10.1016/j.cose.2023.103309.

Pilavakis, N., Jenkins, A., Kökciyan, N. and Vaniea, K. (2023), "'I Didn't Click': What Users Say When Reporting Phishing", doi: 10.14722/usec.2023.233129.

Piščikienė, I., Romeikienė, J. and Šustickienė, B. (2021), "Cyber Vulnerability in Light of Online Learning Reality", *Society Integration Education Proceedings of the International Scientific Conference*, doi: 10.17770/sie2021vol5.6367.

Rantos, K., Spyros, A., Papanikolaou, A., Kritsas, A., Ilioudis, C. and Katos, V. (2020), "Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem", *Computers 2020, Vol. 9, Page 18*, Multidisciplinary Digital Publishing Institute, Vol. 9 No. 1, p. 18, doi: 10.3390/COMPUTERS9010018.

Rumble, J.N. and Irani, T. (2016), "Opening the Doors to Agriculture: The Effect of Transparent Communication on Attitude", *Journal of Applied Communications*, doi: 10.4148/1051-0834.1030.

Sedikides, C., Gaertner, L. and Toguchi, Y. (2003), "Pancultural Self-Enhancement.", *Journal of Personality and Social Psychology*, doi: 10.1037/0022-3514.84.1.60.

Steve, R. (2017), "Office 365 Phishing attacks create a sustained insider nightmare for IT | CSO Online", *CSO UK*, 20 September, available at: https://www.csoonline.com/article/3225469/office-365-phishing-attacks-create-a-sustained-insider-nightmare-for-it.html (accessed 18 December 2021).

Sutter, T., Bozkir, A.S., Gehring, B. and Berlich, P. (2022), "Avoiding the Hook: Influential Factors of Phishing Awareness Training on Click-Rates and a Data-Driven Approach to Predict Email Difficulty Perception", *IEEE Access*, Vol. 10, pp. 100540–100565, doi: 10.1109/ACCESS.2022.3207272.

Wash, R. (2010), "Folk models of home computer security", *ACM International Conference Proceeding Series*, doi: 10.1145/1837110.1837125.

Wash, R. (2020), "How Experts Detect Phishing Scam Emails", *Proceedings of the ACM on Human-Computer Interaction*, Association for Computing Machinery, Vol. 4 No. CSCW2, doi: 10.1145/3415231.

Wash, R. and Cooper, M.M. (2018), "Who Provides Phishing Training?", *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ACM, New York, NY, USA, pp. 1–12, doi: 10.1145/3173574.3174066.

Werlinger, R., Hawkey, K., Botta, D. and Beznosov, K. (2009), "Security Practitioners in Context: Their Activities and Interactions With Other Stakeholders Within Organizations", *International Journal of Human-Computer Studies*, doi: 10.1016/j.ijhcs.2009.03.002.

Zaira, A., Bukhari, Y. and Mehmood, K.K. (2022), "The Mediating role of Effective Communication between Organization Strategy, Structure, Culture and Organization Performance", *Review of Education, Administration & Law*, South Punjab Center for Research and Development (SPCRD), Vol. 5 No. 4, pp. 543–557, doi: 10.47067/REAL.V5I4.289.

APPENDIX I: SCRIPT OF INTERVIEW QUESTIONS

Can you describe your current role and responsibilities in your organisation?

In your experience, what are the most pressing cybersecurity threats organisations face today, and how have these evolved over time?

Could you walk us through the typical process your organisation follows when a phishing attempt is made?

Do you inform the targeted user or the organisation as a whole? Why or why not?

Are there specific criteria that guide these decisions?

What challenges do you face when attempting to communicate phishing threats transparently to end users or stakeholders, and how do you navigate them?

Do you believe employees should be involved or informed during or after a phishing incident?

APPENDIX II: ABRIDGED CODEBOOK

Theme 1: Information Sharing Limitations

Code	Definition	Example Quote	Frequency
Pre-emptive removal	Practitioners remove phishing emails before users see them to prevent accidental clicks.	"If we can remove that e-mail before they (users) ever find out, we will." – P1 (UK)	7/13
No individual notification	Targeted users are not personally informed about sophisticated attacks.	"We don't inform the user personally, we send a generalised advisory." – P6 (India)	6/13
Legal concerns	Reluctance to share info due to GDPR and privacy laws.	"...GDPR privacy...we don't wanna tell the wrong people…" – P10 (UK)	4/13
Reputation protection	Incidents hidden to avoid damaging the company's image.	"We made up a fake story… as it might have impacted the brand…" – P7 (India)	3/13
Consultant constraints	External consultants defer handling to internal teams.	"We wouldn't be the ones that pick it up first." – P11 (UK)	3/13

Theme 2: Prevention Over Response

Code	Definition	Example Quote	Frequency
Prevention focus	Practitioners prefer to eliminate threats rather than inform users post hoc.	"We want to get rid of it as soon as possible… 0% chance of clicking." – P1 (UK)	9/13
Missed learning opportunities	Missed chance to educate users via real intercepted phishing.	"No reason given why we don't show the users once it's resolved." – P10 (UK)	4/13