An examination of organisational cybersecurity support for hybrid workers

Fayez Alotaibi[1,2], Steven Furnell[1] and Christian Wagner[1]
[1] School of Computer Science, University of Nottingham, United Kingdom
[2] College of Science and Humanities, Shaqra University, Saudi Arabia
{Fayez.Alotaibi; Steven.Furnell; Christian.Wagner}@nottingham.ac.uk

Abstract

In 2020, organizations shifted to remote and home working due to COVID-19 restrictions, leading to increased cybersecurity threats as employees operated outside the control of their IT support. Security reports indicated that many employers worried their employees may adopt poor security habits as a result. This study developed two surveys one for employers and one for employees to examine the extent of cybersecurity awareness and support provided in different work environments (e.g., workplace, home, and remote locations). Findings revealed contradictions, as employees' responses often did not align with their employers', particularly regarding cybersecurity support for home and remote work. Some organizations acknowledged that employees had not received adequate cybersecurity support in these settings, highlighting a clear negligence in addressing cybersecurity risks for home and remote workers.

Keywords: Employee awareness, Home Working, Remote Working, Hybrid Working.

Introduction

At the beginning of the COVID-19 pandemic, many organisations asked their employees to work from home (Borkovich & Skovira, 2020). According to CISCO (2020), some organisations in the UK expected that more than half of their staff will continue remotely after COVID-19. However, some workforces were accustomed to work from home or remotely, which led to a rise in cybersecurity challenges (Curran, 2020). In 68% of incidents where data breaches resulted from unintentional actions, human error was a key element (Verizon, 2024). Moreover, according to findings from WifiTalents, 47% of remote workers fell for phishing emails, and it became a high concern for 72% of them. Additionally, 50% used unprotected Wi-Fi networks at least once a week. Employers had not provided sufficient cybersecurity training to 77% of remote workers (Lindner, 2024). However, much of this situation was arguably linked to the rapid and unexpected transition caused by the pandemic, and it is relevant to consider whether (with home working having become a more routine practice since that time) whether organisations and their staff are now better positioned. To have a clear image, this study investigates the extent to which organisations support their employees in three different contexts, namely: workplace, home working and remote working (i.e. public spaces and other locations where neither the employer nor employee have any control over the IT infrastructure). The study also examines the extent to which organisations and their employees believe that they are provided with cybersecurity awareness and related support in their different work environments, and whether they are satisfied with this.

Related works

The shift to home and remote work has been desirable by many organisations since the pandemic of COVID-19. However, this leads to an increase in cybersecurity threats compared to the period before the world crisis, which caused significant security crises among organisations. These changes have raised the level of curiosity among researchers to explore the readiness of organisations toward the shift to home and remote work. Olawale et al. (2024) addressed many security challenges regarding remote workers in terms of security behaviours, security risks and the future of remote working. Cybersecurity Insiders surveyed 413 cybersecurity professionals to investigate the challenges organisations face in terms of humans and technologies. The results show that the most significant challenges organisations could face are cybersecurity awareness and training by (59%), Home/Public WIFI by (56%), and usage of personal devices by (43%)(Schulze, 2020). A report by Tessian (2021), found that around 56% of IT team leaders believed that homeworkers had developed poor cybersecurity behaviours since the transition to remote working. Furthermore, 40% of young remote workers acknowledged making cybersecurity errors while working from home that would go unnoticed by others. Additionally, around 29% of these workforces were hesitant to inform the IT team about their mistakes.

In terms of readiness or action taken by the organisations, Nyarko and Fong (2023) investigate the steps organisations take to keep an acceptable level of compliance among their employees. The study found that most organisations have strategies to ensure acceptable cybersecurity compliance. However, the employees do not know about these strategies or do not receive the required training to comply. Moreover, Mannebäck and Padyab (2021) found four issues regarding remote work security: technical security, security policy, employees' cybersecurity awareness, and readiness for this type of work environment. Georgiadou et al. (2022) assessed the cybersecurity readiness of around 13 European countries toward shifting to remote working mode. The study found that there are several cybersecurity challenges, including the increase in vulnerability to cybersecurity attacks due to the lack of security in the homework environment, inadequate security training, and poor cybersecurity practices.

Research method

In this research, two surveys were developed, one for employers and one for employees. These aimed to investigate the extent to which organisations provide cybersecurity awareness and related support for their employees in different work environments (e.g., in their workplace, at home and when working remotely in other locations) and examine whether both organisations and employees are satisfied with this.

The Employer survey contained 29 questions that covered the following four main themes:

- Background about the organisation itself and staff at the management level.
- Cybersecurity awareness and any related support organisations provide for their employees in different working scenarios.
- Their perception towards their employees' security knowledge and behaviour.
- Their employees 'security practices in different work environments.

The Employee survey contained 28 questions that covered the following four main themes:

- Background about the employee
- Their cybersecurity awareness and any related support provided by their employer for different working scenarios.
- Their perception about this support.
- Their own security practices in different work environments.

Before survey distribution, the associated studies were subject to ethical approval by the University of Nottingham and validated by two external cybersecurity experts. The potential participants were contacted via a number of routes, including via the University of Nottingham business engagement team and the Corporate Partnerships team from the Chartered Institute of Information Security. Moreover, the research team chose 40 UK LinkedIn CEO profiles; a message was sent to each CEO asking them to promote the surveys with their organisations' partners. Also, some overseas organisations were asked to promote the surveys: the College of Sciences and Humanity Studies at Shaqra University, Dawadmi City Airport, King Saud University and The General Commission for Audiovisual Media.

In order to participate in this study, organisations were required to confirm their agreement to participate. Also, organisations must have employees working in each of the three locations. The organisations were asked to share the surveys' links with their employees. Also, they were asked to create a code and share it with their employees, which was then used as an identifier by the management respondents and their employees when completing the surveys. The code allowed the research team to identify the employer and the employee responses originating from the same organisation without knowing the organisation's actual identity. An explanation of how the collected data would be used and how long it will be kept was provided to the respondents. Over the 12 months lifetime of the data collection period, a total of 56 management participants started the survey, along with 133 employees. However, the number was reduced to 7 management responses and 37 employees. The reason for this reduction is that, for data to be usable, there needed to be responses from a management stakeholder and a viable sample of accompanying employees. While several responses were received from management participants, there was an absence of received responses submitted by employees from the same organisation, within the result that a significant proportion of the data collected could not be utilised in the resulting analysis.

A significant challenge with the data collection was the time taken to recruit participants and then for them to secure responses from their employees. Additionally, some agreed to participate but then did not share the survey with their employees. Due to the construction of the study (where it was not possible to see who the participating organisations actually were), the author was not able to followup with the organisations in order to issue reminders or updates on the survey process.

Results

This section compares each employer's responses with those of the respective employees. Fifteen questions were specified as a common factor in distinguishing the convergence of employers and employees. These questions focus on the cybersecurity support that organisations provide to their employees. In the first group of questions, the employers were asked if they provide cybersecurity policies, and employees were asked if they understand these policies. Also, both were asked if these policies permit them to use their devices for work purposes. The second group of questions focuses on the training program and its contents. Employers were asked if they provide training programs that cover three different locations and approaches that are used to deliver the training content. Moreover, Organisations were asked if their training program covered these 12 topics, which will be mentioned in the cybersecurity training section. Additionally, The employer asked to confirm if their employees have received appropriate training in three different locations. Also, the employees were asked to confirm if they feel that their organisation's training program is effective.

The third group of questions focus on the event of a security incident. Employers were asked if they provide their employees with cybersecurity incident plans and access to cybersecurity support at all locations. Also, the employees were asked if they knew how to report a security incident and to whom. Moreover, both employers and employees were provided with a list of security threats that will be mentioned in the cybersecurity thread section. They were asked to tick on the threats that they may encounter in different locations. Furthermore, employers were asked if they think that their employees have received appropriate support, and employees were asked the same question. The fourth group of questions focused on appropriate cybersecurity practices. The organisations were asked to identify which type of employees are better in terms of cybersecurity practice based on their locations. Also, employees were asked if they could deliver their work whilst adhering to the expected cybersecurity behaviours.

In this study, many cases of contradiction were found as, in some cases, the employees' answers did not match their employers' responses, particularly regarding the cybersecurity support provided for home and remote working environments. This section presents two organisations as an example of the most interesting cases among all organisations and the employees' responses, and the reason for this selection is to meet the paper's requirements. In this paper, the code given by each organisation has been replaced with an alphabetical order to keep the organisation's data anonymised as the code was known to the organisations and their employees, as shown in Table 1.

Table 1 Name, Sectors and Number of employees respondents from each organisation

Organisations	Sectors	Employees
A	Education	4
B	Financial and Insurance Activities	5
C	Accounting and Financial Investments	5
D	Education	4
E	Information and Communication	3
F	Financial and Insurance Activities	13
G	Transportation and Storage	3

In order to identify the average of employees in each question, each score was given values from 1 to 5, as shown in Table 2, which also shows the color-coding used in later tables (Note: any not applicable responses were excluded during the resulting analysis and the average of the employees counted based on the responses that were received). These scales are used to identify the average of employees' agreement scores in each question, and the table shows the associated color-coding that is also used in the presentation of later results.

Table 2. Numeric Scales and Colour Coding

5	Strongly Agree	4	Agree	3	Neutral	2	Disagree	1	Strongly Disagree

Cybersecurity policies

In terms of cybersecurity policies, organisation agrees that it provides a clear cybersecurity policy for their employees. Also, the average of the employees matches their employer's score except for the remote work location, as shown in Table 3. Moreover, the same situation is repeated in organisation F, but this time in the home environment. It can be observed that most employees are not sure if their organisation's policy covers home and remote work locations. This could be due to the following reason: there may be policies, but the organisations have not specified which rules should be followed in each location. Without clear guidelines, employees may fail to comply with a policy that lacks best practices regarding the work environment. As a result, this could negatively impact employees' cybersecurity behaviours.

Table 3 Employer vs Employees Regarding Security Policy in Org E and Org F

	Org E			Org F		
	Work	**Home**	**Remote**	**Work**	**Home**	**Remote**
Employee (avg.)	4.3	4	3.6	4.2	3.3	4.3
Employer	5	5	5	5	5	5

Policy permission. Table 4 shows that organisation B strongly agrees that the security policy permits their employees to use their devices for work purposes. However, the employee's section tells something different especially at home and remote locations. In terms of organisation C, both employer's and employees' responses meet each other. Allowing employees to use their personal devices can lead to data breaches if they are uncontrolled by IT teams. These devices may be used for personal activities, which can expand the circle of cybersecurity risks, including fraud and other related threats. According to Schulze (2020) 61% of IT managers believe that remote workers are more likely to use the same device for work and other personal activities.

Table 4 Using personal devices at all locations in Org B and Org C

	Org B			Org C		
	Work	**Home**	**Remote**	**Work**	**Home**	**Remote**
Employee (avg.)	4.6	3.6	3.6	4.2	4	4
Employer	5	5	5	4	4	4

Training programs

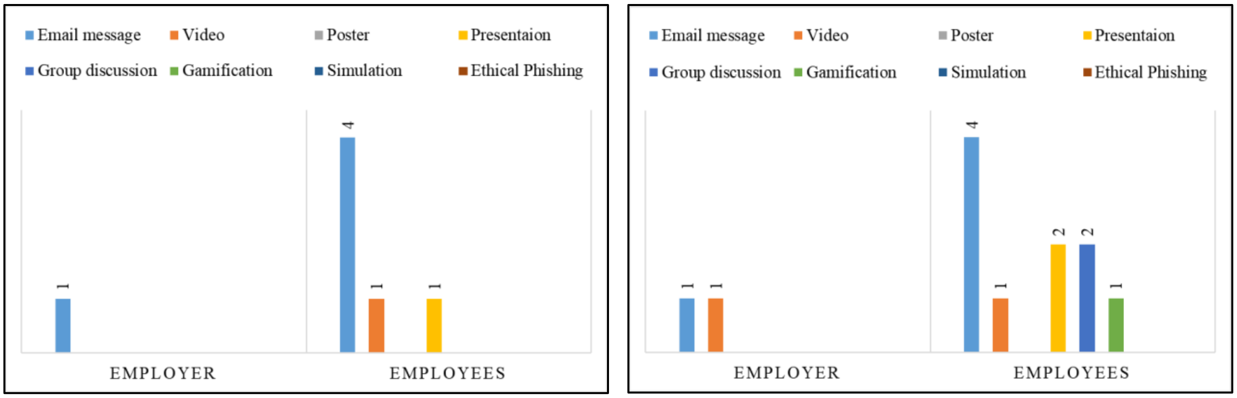
In terms of training and education, Table 5 illustrates that organisation A agrees that they provide an educational program that covers all locations. However, the average of the employee's score does not meet their employer's score at all locations. Moreover, the average of employees in organisation D does not meet their employees' scores in terms of workplace and remote working. Both employers and employees provide almost the same score in terms of home working as shown in Table 5.

It seems that the majority of employees are unsure whether their organisation's training program covers all locations. This may be because the training contents tend to be more general than specific, for example, teaching them how to behave in general rather than how to behave in each location. Another reason is that the training contents are insufficient to cover some security topics, especially those related to all locations, as shown in Table 6.

Table 5 Training program covers three locations in Org A and Org D

	Org A			Org D		
	Work	**Home**	**Remote**	**Work**	**Home**	**Remote**
Employee (avg.)	3	3.6	3.5	3.2	2.75	3
Employer	4	4	4	5	3	4

Training approaches. Employers and employees were provided with a list of approaches identified by our research literature, as shown in Figure 1. The reason is to check if the organisation used different methods to meet their employees' preferences. As shown in Figure 1, email messages are only the approach used by organisation D, and the majority of employees also confirmed that. In terms of organisation A, the employer believes that email messages and videos are the only approaches used. However, the employees have different opinions based on what they have experienced. It seems that the management team at the high level are not aware of the methods used by their trainers, as evidenced by their employees' answers. Let's assume they only use what they provide. Do these approaches meet all employees' preferences? Abawajy (2014) suggested that using multiple awareness delivery methods is better than using one.



(a) (b)

Figure 1 The approaches used in training programs in (a) Org D and (b) Org A

Cybersecurity Topics. A list of 12 cybersecurity topics was provided to both employers and employees. They were asked for their agreement on which extent their organisation programmes cover these topics. These were provided by our previous study (Alotaibi et al., 2023), presented in Table 6. Table 6 shows that orgnisation D agreed that their training program covers most of the security topics except some topics; they neither agreed nor disagreed if their training program covers removable media, remote working security and (BYOD). Additionally, the average number of employees agreed with their employees on most of the topics except two: incident management plan and security at home. However, it is higher than their employer's score regarding BYOD, removable media and remote working security. It also shows that orgnisation E agreed that all 12 topics are covered by their training program. However, the average number of employees is low regarding eight topics. The possible reason for this contradiction is that some of these topics may have not been covered enough. For example, they may inform them about the importance of reporting security incidents, but they may not teach them how to report an incident. Telling employees what to do is not enough; organisations should teach them how to do it.

Table 6 Cybersecurity topics covered by the training program in Org D and Org E

Org D			Org E		
Security topics	Employer	Employee (avg.)	Security topics	Employer	Employee (avg.)
Security Threats	4	3.75	Security Threats	5	4.3
Passwords & Authentication	5	4.5	Passwords & Authentication	5	4.3
Backup and Recovery	5	3.75	Backup and Recovery	5	3
Network Security	5	4.25	Network Security	5	3.6
Device Care	4	3.75	Device Care	5	3.6
Updating Software	4	3.75	Updating Software	5	3.6
Security tools/services	Non	3.75	Security tools/services	5	3
Incident Management	5	3.25	Incident Management	5	4.6
Bring your own Device	2	3.75	Bring your own Device	5	3.6
Removable Media	3	3.5	Removable Media	5	4
Security at home	4	3.25	Security at home	5	3.6
Remote working security	3	3.5	Remote working security	5	3.3

Appropriate training. Table 7 shows that Organization E strongly agrees that their employees received appropriate training at all locations. However, the employees have an opinion. The same situation has been repeated in organisation F, where the employer says something, and the employees say something different. It seems that most of the employees are not sure if they have received appropriate training for all locations. This is could a reflection of the quality of their organisation's cybersecurity training programs. Another reason the training content may not be regularly updated, employees may see the same content again and again, which may make them uncertain about the effectiveness of the training program. Organisations should assess their training program regularly to determine whether it is effective or not.

Table 7 Employees receive proper training in Org E and Org F

	Org E			Org F		
	Work	**Home**	**Remote**	**Work**	**Home**	**Remote**
Employee (avg.)	3.6	3.3	3.6	3.4	3.3	3.4
Employer	5	5	5	4	4	4

Cybersecurity incident plans.

A cybersecurity incident or response plan can be identified as a list of steps followed by organisations and their employees in the event of a cybersecurity incident. Both organisations and their employees were asked two questions, which are as follows:

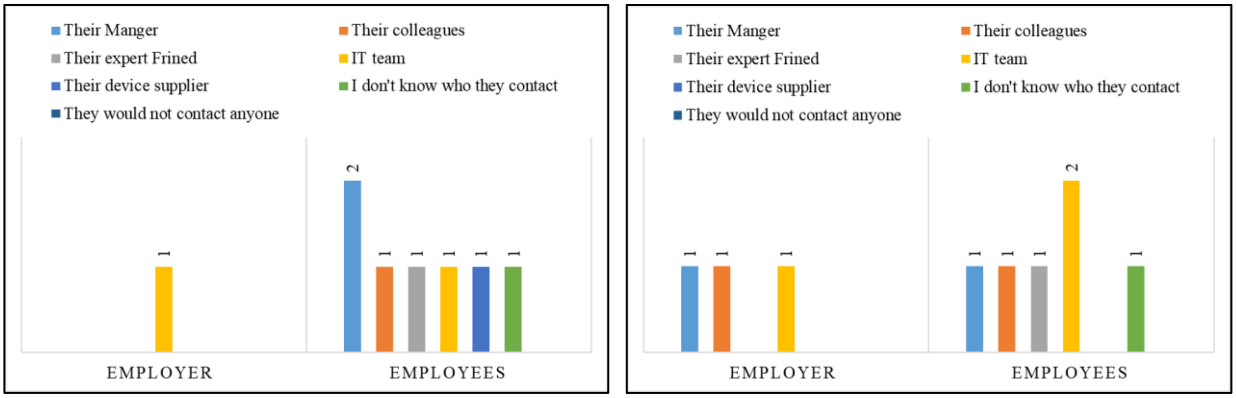
- Do you provide your employees with a cybersecurity incident plan that covers workplace, home, and remote working? (Employer)
- Do you have a clear understanding of how to report security incidents or concerns? (Employees)

As shown in Table 8, organisations A and D agreed that they provide a cybersecurity Incident plan that covers the three locations. However, the average of the employees was very low compared to their employers' scores at all locations. It seems that most employees are not sure how to report an incident. An unclear cybersecurity incident management plan can leave employees uncertain about the steps to take, which may even lead them to ignore the incident.

Table 8 The organisation provides an incident plan in Org A and Org D

	Org A			Org D		
	Work	**Home**	**Remote**	**Work**	**Home**	**Remote**
Employee (avg.)	3	3.3	2.5	3.25	3	3
Employer	5	4	4	5	4	4

Event of cybersecurity incident. A list of people and options were provided, as shown in Figure 3. Both organisations and their employees need to choose from the list. Organisation A suggested that employees need to contact IT teams within their organisation. However, the employees have different answers, as almost each of them chooses a different person. It seems that most of the employees are unsure of whom they should contact. Organisation G suggested that employees should contact their manager, colleagues, and IT teams in the event of a cybersecurity incident. As shown in Figure 3, most of the employees' answers match their employer's answers except two employees. One of the employees chose to contact his/her expert friend, and the other employee said he/she didn't know who should contact. This is more evidence to confirm that an unclear security incident plan could make employees uncertain of how they should behave during the incident.t.



(a) (b)

Figure 2 People to contact in security event in (a) Org A and (b) Org G:

Access to security-related support. Table 9 shoes that, Organisation G agreed that they provide access to security related support for their employees at the workplace. However, they neither agreed nor disagreed in terms of home and remote working. In terms of employees, all the employees have the same point of view about all allocations. In terms of organisation D, they agree that they provide their employees with access to security-related support at all locations. However, the average of employees is lower than the score given by their employer for all locations, as shown in table 9. If the employees do not have access to security-related support, how will they respond to cybersecurity threats, and from whom should they seek advice? This is also can be included under the impact of having an unclear cybersecurity incidents plan.

Table 9: The organisation provides security access for employees in Org G and Org D

	Org G			Org D		
	Work	**Home**	**Remote**	**Work**	**Home**	**Remote**
Employee (avg.)	4.3	3.6	3.6	3.50	3.5	3.5
Employer	5	3	3	5	4	4

Security behaviour

In terms of employees' cybersecurity behaviours, Both organisations C and F neither agreed nor disagreed about their employees' cybersecurity behaviour in all locations. Also, the organisation's C employees were unsure if they could deliver an accepted cybersecurity behaviour when they work remotely. However, organization F employees believe they could deliver good security behaviour. Moreover, the average number of both organisations' employees shows that they are able to provide good cybersecurity behaviours at the workplace and at home, as shown in Table 10.. It seems that organisations are not fully aware of their employees' behaviour, and poor cybersecurity support can lead to poor cybersecurity behaviour. Providing training programs and policies to increase employees' awareness is not enough; employers also need to monitor their employees' behaviour to assess the effectiveness of the support provided.

Table 10 Rating employees' security behaviour in Org C and Org F

	Org C			Org F		
	Work	**Home**	**Remote**	**Work**	**Home**	**Remote**
Employee (avg.)	4	3.75	3	4.8	4.8	4.6
Employer	3	3	3	3	3	3

Security support in general

As shown in Table 11, organisation D agreed that their staff have been supported appropriately at the workplace. However, they disagree in terms of home and remote working. In terms of the employees, the average of employees shows that they agreed with their employer in terms of the workplace. However, they neither agree nor disagree in terms of home and remote working, which is above their employer score. The case also repeated in terms of organisation G. The result shows that there is a need to support both home and remote environments as these types of workforces may adopt unacceptable security behaviours with the absence of security support at home and remotely.

Table 11 Employees receive proper support in Org D and Org G

	Org D			Org G		
	Work	**Home**	**Remote**	**Work**	**Home**	**Remote**
Employee (avg.)	4.2	3.25	3.25	4.3	3.3	3.3
Employer	5	2	2	5	3	3

Security threats

A list of cybersecurity threats was provided to organisations and employees to identify which of these threats the employees may face at work or at home. To make it easy for them, the author provided four statements that both can agree with. For example, when the author provides cybersecurity threats such as Phishing emails, then organisations need to choose one or more of the following statements:

A. They may face this threat at home.
B. They may face this threat at work
C. They may not face this threat.
D. They may not be familiar with this threat.

In terms of the list of cybersecurity threats, they both were provided with types of threats, which are as follows:

- Phishing emails
- Social engineering
- Network attack
- Application attack
- Ransomware and Malware

As shown in Table 12, organisation A believed that their employers may face all of the cybersecurity threats at work only, except phishing and ransomware, which they may face at both work and home. However, the majority of the employees believed they may face all the threats at home, and most of them are not familiar with these threats. Moreover, organisation C believed that their employees may face all threats at home and in the workplace except application attacks, which their employees may not be familiar with. However, the majority of the employees think that they are not familiar with all these threats.

Table 12 Threats employees may face in Org A and Org C

Org A						Org C					
Attack types	Audience	A	B	C	D	Attack types	Audience	A	B	C	D
Phishing emails	Employer	✓	✓	-	-	Phishing emails	Employer	✓	✓	-	-
	Employees	2	1	-	1		Employees	1	1	1	2
Social Engineering	Employer	-	✓	-	-	Social Engineering	Employer	✓	✓	-	-
	Employees	2	-	-	1		Employees	-	-	2	2
Ransomware and Malware	Employer	✓	✓	-	✓	Ransomware and Malware	Employer	✓	✓	-	-
	Employees	1	-	-	2		Employees	1	1	1	2
Network attack	Employer	-	✓	-	-	Network attack	Employer	✓	✓	-	-
	Employees	1	1	-	2		Employees	1	1	1	2
Application attack	Employer	-	✓	-	-	Application attack	Employer	-	-	-	✓
	Employees	1	2	1	2		Employees	1	1	1	2

Discussion

The investigation found that there are many cases of contradiction between the employers' responses and the employees' responses within the same organisation, as shown in Table 3 and 4. For example, while organisations E and F claimed that they provide cybersecurity policies that cover all locations, the employees' responses say something else, especially in terms of home and remote workers. This gives a first impression that the employer and the employees are not on the same page. Based on the employer responses, there could be a policy, but this policy might lack clarity or comprehensiveness regarding home and remote working. Otherwise, employees would not respond with neutrality. This pattern is also repeated in the other aspects of the questions.

Moreover, there are also contradictions within the employers' responses across various questions. For example, organisation D agreed that they provide cybersecurity training for remote workers as shown in Table 5. However, when they were asked if their training program covered the topic of remote working, their answers were inconsistent. Additionally, as shown in Table 6 and Figure 1, the organisation's training programs may not be effective as some security topics were not covered. Furthermore, they relied on a single cybersecurity awareness approach, whereas using multiple delivery methods is generally more effective.

Furthermore, it was notable that some organisations were not confident when their responses were compared. For example, organisation A agreed that they provide a clear incident plan, but when their employees were asked about who they would contact in the event of a security incident, almost each of them chose a different person. Organisation E appears to be confident about its training program's effectiveness. However, the majority of the security topics were not fully covered based on the employees' responses. Organisation F claimed that their employees had received proper training. However, they were uncertain whether their employees could maintain expected security behaviour. This raises an important question: How can they not be confident about their employees' behaviour if they believe their employees have received proper training?.

Additionally, organization C appears to be not confident about their employees' security behaviour, as shown in Table 10. However, their security policy allowed the employees to use their personal devices for work purposes, as shown in Table 2. The question here is if the organisation is not confident about their employees' behaviour, then why do they allow their employees to use their own devices?, as these devices may be used for personal activities. According to Schulze (2020) 61% of IT managers believe that remote workers are more likely to use the same device for work and other personal activities. Moreover, organisation G appears to be uncertain if they provide their employees with access to security-related support at home and in remote locations. Additionally, they were not sure if their employees received proper security support in general. The question here is what the organisation expects from their employees in terms of security.

Furthermore, most employees and employers agreed that employees may face all the cybersecurity threats mentioned in the previous section. However, the majority of the employees believe they may not be familiar with some of these threats. The question here is, if the employees are not familiar with some of these threats, how will they be able to deliver the expected cybersecurity behaviour?, teaching workforce to detect cybersecurity threats will help them to avoid these risks (CMA, 2021).

Overall, the findings reveal that there is a variation in whether cybersecurity policy and provision are sufficiently addressing the different contexts in which staff may find themselves working and also that what organisations believe themselves to have addressed will often not align with what staff understand or remember. Both aspects highlight the need for a more holistic and robust approach.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & information technology*, *33*(3), 237-248.

Alotaibi, F., Furnell, S., & He, Y. (2023). Cyber security awareness and education support for home and hybrid workers. International Symposium on Human Aspects of Information Security and Assurance,

Borkovich, D. J., & Skovira, R. J. (2020). Working from home: Cybersecurity in the age of COVID-19. *Issues in Information Systems*, *21*(4).

CISCO. (2020). *Futuer of secure remte work report*. CISCO Secure. Retrieved 16 October 2024 from https://www.cisco.com/c/dam/global/en_uk/products/security/pdf/cisco-emea-report-2020_fa_final.pdf

CMA. (2021). *Best cybersecurity tips for remote workers*. https://www.cm-alliance.com/cybersecurity-blog/best-cybersecurity-tips-for-remote-workers

Curran, K. (2020). Cyber security and the remote workforce. *Computer Fraud & Security*, *2020*(6), 11-12.

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*, *35*(2), 486-505.

Lindner, J. (2024). *Remote work cybersecurity statistics: alarming trends revealed by recent data*. Wifitalents. Retrieved 16 October from https://wifitalents.com/statistic/remote-work-cybersecurity/#sources

Mannebäck, E., & Padyab, A. (2021). Challenges of managing information security during the pandemic. *Challenges*, *12*(2), 30.

Nyarko, D. A., & Fong, R. C.-w. (2023). Cyber security compliance among remote workers. Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability, London, September 2022,

Olawale, O., Ajayi, F. A., Udeh, C. A., & Odejide, O. A. (2024). Remote work policies for IT professionals: review of current practices and future trends. *International Journal of Management & Entrepreneurship Research*, *6*(4), 1236-1258.

Schulze, H. (2020). *Remote workforce security reporte*. Cybersecurity Insiders. Retrieved 16 October 2024 from https://pages.bitglass.com/rs/418-ZAL-815/images/CDFY20Q2RemoteWorkforceReport%282%29.pdf?aliId=eyJpIjoiM3JOXC8yWENvbk8yZ2tyUE8iLCJ0IjoienhMa3IwWVFCNXVDVXpYaEVGZTdGUT09In0%253D

Tessian. (2021). *Back to work security behaviors report*. Tessian. Retrieved 16 October 2024 from https://f.hubspotusercontent20.net/hubfs/1670277/%5BCollateral%5D%20Tessian%20Research/%5BTessian%20Research%5D%20Back%20to%20Work%20-%20Security%20Behaviors%20Report.pdf?__hstc=&__hssc=&hsCtaTracking=71dec6fb-2272-456b-837a-7195d1a57810%7Ca5ded5ee-007a-4cbc-9073-740f99d30985

Verizon. (2024). *Data breach investigations report*. Verizon Business. Retrieved 16 October 2024 from https://www.verizon.com/business/resources/Tb8f/reports/2024-dbir-data-breach-investigations-report.pdf