What Influences People's View of Cyber Security Culture in Higher Education Institutions? An Empirical Study

Tai Durojaiye
Information Security Group
Royal Holloway University of London
Egham, Surrey, United Kingdom
Email: Tai.Durojaiye.2019@live.rhul.ac.uk

Konstantinos Mersinas
Information Security Group
Royal Holloway University of London
Egham, Surrey, United Kingdom
Email: Konstantinos.Mersinas@rhul.ac.uk

Dawn Watling
Department of Psychology
Royal Holloway University of London
Egham, Surrey, United Kingdom
Email: Dawn.Watling@rhul.ac.uk

***Abstract*—The education sector is considered to have the poorest security culture score amongst many sectors. Human aspects of cyber security including cyber security culture which have often been overlooked in the study of cyber security have not been fully explored in Higher Education Institutions (HEIs). The lack of understanding of cyber security culture, unclear definition of the concept and guidance on how to measure and foster it, are challenges HEIs face. To address this lack of knowledge and understanding, we explore the factors that influence people's view of cyber security culture in UK HEIs. We interviewed senior HEI leaders, academics, professional services staff, and students (19 participants in total) in three UK universities of similar characteristics. We find that communication necessary to influence security culture in HEIs is lacking. There is lack of policies/frameworks in place to guide user behaviour. We also observe that IT expectations are not well defined, and phishing exercises create problems between the IT team and users. There is no onboarding security training and awareness for students which make up the largest percentage of the HEI populace. We recommend that senior HEI leaders invest in training and awareness programmes for IT staff and other users, focusing on communication, engagement, collaboration, and social engineering. We also recommend that senior HEI leaders prioritise the creation and implementation of a cyber security strategy, on which policies and other security efforts could be based. The adoption of these recommendations could influence the mindsets of users towards engaging in safe cyber security behaviours and by doing so improving the culture of security in HEIs.**

Keywords- Cyber security culture; Higher Education Institutions (HEIs); security behaviour; communication; phishing; training.

I. INTRODUCTION

The increasing use of technology in the twenty-first century continues to yield huge benefits to nations, organisations, and individuals in their day-to-day activities. Modern technological advancements such as Artificial Intelligence (AI), Internet of Things (IoT), big data, 5G, cloud computing and blockchain have affected different areas of society [1][2]. The application of these technologies has brought improvements to different industry sectors, ranging from medical to education. However, the reliance on technology also has its challenges. The application of the technological advancements in different domains translate into more data being generated. With the increase in the attack surface (that is, the total of all exposures of an information system) [3] due to the abundance of data generated, organisations become easy targets for cyber attacks.

Huge volume of data has caused organisations and users to be prime targets for cyber attacks and hackers [4]. Cyber attacks use innovative approaches. Cyber attacks and hackers use different methods, and in some instances, they use advanced technology to prevent staff and students from gaining access to the needed data and networks. This is a major threat in HEIs, where the availability to information could be denied by cyber attacks [5]. According to [5], most UK HEIs are not well prepared to defend their human and information assets from breaches, phishing attacks, and other security vulnerabilities.

Users continue to pose a threat to the information assets of HEIs. As the PwC Information Security Breaches Survey [6] reports, three quarters of large organisations suffered staff-related security breaches while for small businesses it was one third, a respective percentage rise of 17% and 9% from 2014 to 2015. When organisations were questioned about the single worst breach suffered, 50% attributed the cause to inadvertent human error. This was a percentage increase of 19% from 2014 to 2015.

Human error can be attributed to accidents or negligence. The importance of paying attention to human error is further corroborated by the IBM survey which states that nine out of ten information security incidents are caused by some sort of human error [7].

Thus, it is reasonable to hypothesise that human factors constitute a challenge for HEI leaders too. The approach many organisation leaders have taken to reduce the risk posed by cyber threats is focusing on and increasing their investments on technical controls [8]. Traditionally, the focus of risk mitigation in information security has been on technical solutions. Despite following this approach to defend the organisation ecosystem, cyber security breaches have not declined [9]. While technical solutions offer some protection, it is not a panacea for all cyber security breaches. Hence, this calls for additional defence to be employed [10].

Over the years the approach to information security has evolved and gone through many stages. As study [11] shows, the information security evolution moved from the

 ISBN: 978-1-61208-893-8

initial stages where information security was characterised solely by technical approach, best left for technical experts [12] to a stage where efforts were made to understand and address the human element as an essential security factor [13].

The industry is now at a stage where researchers and organisations are becoming more aware of the importance of the often-overlooked area, that is, the human aspect of cyber security with emphasis on Cyber Security Culture (CSC). This stage is characterised by researchers defining CSC, identifying, and attempting to address the gaps that exist in the domain [14]. Although there are studies that indicate associations between CSC and characteristics such as attitudes and social norms, there are only indirect associations between CSC and secure behaviour [15].

While some organisations have different training and awareness programmes in place, a study of CSC definitions [16] shows the ineffectiveness of security awareness and education demonstrating that training itself is not enough. Therefore, more research is required to gain a deeper understanding of the human aspect of cyber security.

An understanding of CSC will provide an insight which could be used to address users' unsafe security behaviours. There are gaps that have been identified based on extant literature on CSC, which argue that the field lacks guidance on how to foster it. For instance, the descriptive and theoretical solutions offered by researchers can be impractical to apply in organisational settings, tool validation is needed, and guidelines and practices are needed for developing and implementing security culture in organisations. Also, a gap exists between awareness levels, respective practices, and behaviour [16]. Security culture improvement is needed in organisations to maintain a healthy posture.

Importantly, there are limited empirical studies on CSC in HEIs. Cyber security culture is ill-defined and there are no clear guidelines on how to foster security culture. The education sector lacks understanding about this important domain. The consequence of this is that users exhibit certain security behaviours which make their institution a prime target for cyber attacks. If we know personnel and students' perception of CSC, then we will better understand why they exhibit such security behaviours which put their institutions at risk of cyber breaches.

In this paper, we focus on CSC in the education sector. Our aim is to explore what influences personnel (senior management members, academics, professional services/ administrative staff) and students' views of CSC in HEIs. It is when we understand what is happening in this domain and in this environment, that effective strategies, methods, and appropriate course of action could be proposed and taken to defend information assets in the institutions. Then, plans could be made to instil security behaviours in people which will lead to a healthy security posture in HEIs.

II. BACKGROUND AND IMPORTANCE

The sector is an attractive target for ransomware attacks enabled by phishing operations. Many HEIs around the world and in the UK suffer from cyber attacks on a regular basis. A Joint Information Systems Committee (JISC) report [17] indicates that UK HEIs are not well prepared to defend themselves and recover from cyber attacks if and when they happen. In a survey of CSC in 17 industry sectors, distributed across 24 countries, the Security Culture Report [18] confirms that the education sector has the poorest security culture score among other poor performers such as transportation and energy and utilities.

The education sector continues to be an increasingly attractive target for cyber attacks because of the wealth of information repositories it holds. Information ranges from intellectual property to information about staff, students, and alumni. Cyber attacks in UK HEIs are increasing and are becoming more targeted at users in this sector because of its poor security culture. Indicatively, breaches have been reported at University of Greenwich [19], and University of Edinburgh [20]. This could lead to financial and indirect losses, such as reputational damage, cost of containing the breach, etc. The security solutions that have often been proposed and offered by organisations and security professionals have little or no involvement with users. With a new perspective, we make some recommendations.

We identified three UK universities with similar characteristics to conduct interviews. In the next section, we discuss our research methodology.

III. CURRENT STATE OF CYBER SECURITY CULTURE

CSC studies have been conducted in different sectors, such as banking and finance, healthcare, and government organisations. CSC related work has focussed on the definitions of information security culture (ISC) and CSC, with the two considered to be similar. Although, there are similarities between ISC and CSC, there is no universally agreed definition of CSC [16].

Researchers have also developed models and frameworks to provide guidance in the understanding of CSC. Some of these have built on Schein's iceberg model of organisation culture [21]. The STOPE framework [22] have been used as a basis to develop another framework such as the Information Security Culture Framework (ISCF) in [23].
Other areas that are important for building and maintaining CSC are management support or involvement, security awareness and training, security policy, communication and change management [24]-[30].

Some of the existing solutions that have been offered are theoretical and conceptual in nature, mainly geared towards industry and not HEI-focussed. The solutions are not adequate for fostering CSC in industry nor in HEIs. Hence, there is the need for some of the solutions to be tested through empirical studies. To the best of our knowledge,

there is a lack of empirical studies focusing on the cyber security posture of UK HEIs. In view of the inadequate solutions, we investigate the perceptions of personnel and students of CSC in UK HEIs.

Our goal is to highlight the current problems in UK HEIs through a practical approach, allowing pertinent issues of security culture to emerge. Findings could then be used by researchers as a basis for further CSC investigations in UK HEIs and beyond.

IV. METHODOLOGY

We approached staff in three HEIs, all located in the south of England, that were considered similar in terms of student numbers (between 10,000 and 20,000) and staff numbers. The websites of the three UK universities were used to contact participants (N=19) that fit the criteria of our target group, resulting in interviews with three senior management members, six academics (three of whom have information security background), seven professional services/administrative staff, and three PhD students.

Interviews started with general questions on the role and responsibilities of the interviewee [31][32]. Questions included security perceptions, governance, devolution, university structure and culture. Other questions focused on training and development, security of information and records.

To understand what influences personnel and students' views of CSC, we conducted semi-structured interviews, with questions designed and conducted by a multidisciplinary team of three researchers.

One-to-one interviews were conducted between 29 January 2020 and 21 July 2020. Sixteen interviews were conducted face-to-face while three were done online. The interview duration was approximately 30 minutes. Participant's personal identifiable information was anonymised during data cleaning by one of the researchers and were therefore unidentifiable for the other researchers.

Interviews were recorded, transcribed, and then analysed. Content analysis of the interviews, based on the approach described in [32]-[34], was conducted with support of NVivo software. In total 1961 statements were identified.

We focus on the individual level of the security culture model presented in [11]. The individual level of the model focuses on user attributes and characteristics which impact security attitude and behaviour. We make the model more comprehensive by adapting it to cover more factors related to the user's internal-driven individual notions which affect their security attitude and behaviour. Other relevant dimensions are identified from [18] and the comprehensive model is presented in Figure 1. The individual level is further broken down into the seven dimensions of CSC. The definitions of the dimensions are as shown in TABLE 1. DIMENSIONS OF CYBER SECURITY CULTURE. From the detailed analysis of our interviews, themes, that is, recurring topics emerge.

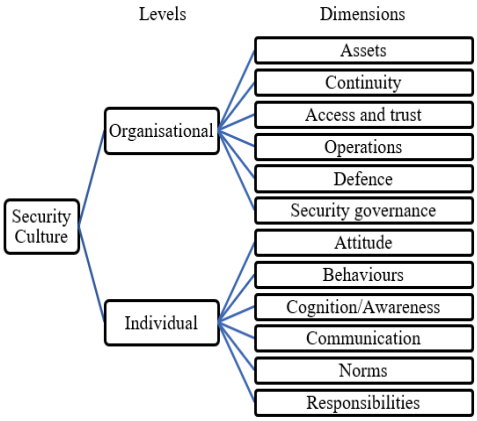

Figure 1. A Comprehensive Security Culture Model [11]

TABLE 1. DIMENSIONS OF CYBER SECURITY CULTURE [18]

Dimension	Definition
Attitude	The feelings and beliefs that employees have toward the security protocol
Behaviours	The actions and activities of employees that have direct and indirect impact on the security of the organisation
Cognition/ Awareness	Employees' understanding, knowledge, and awareness of security issues and activities
Communication	The quality of communication channels to discuss security-related topics, promote a sense of belonging and provide support for security issues and incident reporting
Compliance	The knowledge of written security policies and the extent that employees follow them
Norms	The knowledge of and adherence to unwritten rules of conduct in the organisation
Responsibilities	How employees perceive their role as a critical factor in sustaining or endangering the security of the organisation

V. RESULTS

From the analysis of the 1961 interview statements identified within the 19 interviews, Condensed Meaning Units (CMUs) were generated. A CMU is the shortened version of an interview statement that retains the primary meaning. The relevant CMUs related to CSC dimensions (TABLE 1. DIMENSIONS OF CYBER SECURITY CULTURE) were grouped into codes and were labelled in relation to their content or context; thus, allowing the formation of categories. From the categories, six themes, which reveal underlying meanings, emerge. The themes are: communication; policies and frameworks; IT expectations; moving away from phishing exercises; training, reinforced training and awareness; and CSC measurement.

 ISBN: 978-1-61208-893-8

In this section, we present our findings and the emerging themes from the qualitative analysis; indicative interview excerpts are provided for each finding.

A. Communication

Communication is the main emerging theme in this study that underpins all other themes. Communication is a vital tool which must be mastered and used effectively in collaboration, relationship building, policy conveying, awareness raising and training. The key categories from the study which contribute to the emergence of this theme are communication improvement, beneficial outcomes of collaboration, communication, and information management. The latter captures poor and impersonal communication with users and consists of unclear university cyber security plans, which are poorly communicated with users.

1) Communication Finding 1: Lack of systematic communication from the IT team to users

Communication problems exist in HEIs. As an interviewee explains “there is a lack of systematic communication between the IT services regarding cyber security to staff in general”. IT communication is seen as unclear and opaque, and because of this, users have had to form their own judgements based on the little or no information they have about security. The following indicative extracts support this: “I don't even know that. So, I would just like them to be a bit more clear”; “So I feel there's a real [problem], everything is very opaque”. While another interviewee understands that the IT team could be busy because of other priorities, they state “They have priorities and that security, because I don't hear about any of this stuff. I don't know. So, I formed judgements because I don't have information”.

The following extracts demonstrate the lack of communication from the IT team to users: “I don't think there is enough communication. That's my big thing, just not communicating enough”. An interviewee explains the need for the IT team to listen more “I think that generally our IT department do a very good job of communicating, but we don't always do a very good job of listening”.

Further, as another user indicates there is a lack of transparency from the IT team: “[IT] haven't told us anything about it. They don't tend to tell us stuff about that. So yeah, maybe they could communicate with us better about what they are doing”. Hence, users demand for more communication. An interviewee suggests that communication from the IT team needs to be refined “And clearly they are monitoring phishing emails, and they are sending reminders to people. So ‘don't click things’ and so on. Let's forget if that is a correct reminder because you can't actually tell people not to click the link [..]. It's part of the job”. Thus, there is a query on how people can even do their work if such information is being promulgated without an alternative solution being offered.

Participants highlighted the specific need for pre- and post-phishing communication where phishing exercises have been planned. An interviewee sums this up: “I feel like there should be a message to say like, [..], this was a phishing test” and on post phishing exercises communication “but then definitely there needs to be a clear explanation afterwards as to why they did that and then how students should react and what would be beneficial for them to do in that situation”.

2) Communication Finding 2: Collaboration problems exist between the IT team and academics

An observation made is that there are collaboration problems, where academics’ offer of their cyber security expertise and this is not embraced by the IT team, as the following extracts indicate: "I try to work with them and to offer help and to try to increase the level of communication and collaboration, that has proved to be difficult". This signifies a challenge in information sharing between academics and IT staff.

3) Communication Finding 3: Communication is impersonal

Another finding from our study indicates that communication is impersonal. There are no names on emails received from IT services. An interviewee says, “I don't like the fact that [..] you don't ever get a signature, you have a conversation with someone over a few emails and you don't know who you're talking to”.

B. Policies and Frameworks for Guiding Cyber Security Behaviour

This theme is concerned with the need to have policies and frameworks in place to guide the cyber security expectations and behaviours of HEI information asset users. The policies cover behaviour sets that influence how people practice cyber security. The behaviour sets are compliance with security policy, intergroup coordination and communication, phishing email behaviour, and password behaviour [35]. The policies act as guide for users (including IT staff) in their daily use of information assets and interactions with other users and technology. It also covers regulatory, legal, and compliance information, including General Data Protection Regulation (GDPR).

Our aim is to assess personnel and students’ perception of the policies and frameworks that are in place and their impact on influencing user behaviour towards security compliance.

1) Policies and Frameworks Finding 1: Lack of enough policies/frameworks

Our findings show that enough policies and frameworks are not in place for guiding user behaviour in HEIs. With reference to policies and processes that are specific to cyber security an interviewee states “I don't think there are enough, policies and processes in place that people would want to work around it". An interviewee does not feel the HEI security policy defines the boundaries through which they operate, “there is nothing to stop me sending a personal email from my work account, so we don't have anything, I believe, in our terms or policies that prevent you from doing

that". Further, another interviewee says, "there is too much writing of policies and not enough doing it", suggesting a lack of policy implementation.

The policies that are in place are not communicated effectively to students and staff. Policy information is shared via employment contract suggesting a passive approach of communication. An interviewee comments "..a lot of it is covered by individual employment contracts with us, or student enrolment with us in those different areas, as to the standards that [we are] required to meet and what they can and can't do with our network and our information assets".

2) Policies and Frameworks Finding 2: Lack of prioritisation

Prioritisation is another problem identified through this research. For instance, an interviewee comments: "I think one of the challenges [the university] has had around cyber security is that it has tried to do everything in terms of policy standard and technology all at once without any real sense of priority and without any real sense of priority based on an intelligent assessment of what the actual threat and risk is". While another interviewee states "Is it in a framework, is it written down? Can I put my hand on it and say, in priority order, these are the most critical data sets and services to the running of this organisation, you know, prioritise these for security and resilience over others? No. I don't think there is"

C. IT Expectations

This theme is about the need for the IT team to engage more with users to understand the challenges that they face in terms of not knowing what is expected of them. The scope of the theme relates to compliance and non-compliance with IT expectations. Its purpose is to explore users' attitude and behaviour towards compliance with IT expectations.

1) IT Expectations Finding 1: IT Expectations are not well defined

IT expectations are not defined clearly. An interviewee says, "that sounds a little bit weak because the expectations are probably not very well defined, as I probably mentioned there is a lack of systematic communication between the IT services regarding cyber security to staff in general". This finding also demonstrates that there is a link between IT expectations and communication.

2) IT Expectations Finding 2: Academics do not see the need for IT compliance

An interviewee comments about the attitude of academics towards compliance, "I think academic ones, they often don't see why they should and don't understand the implication of what they're doing. And you get that in other things like financial regulations and HR regulations as well. They just think that it's getting in their way. They've got things to do and it's the silliness, and they don't understand really the serious implications of what they're doing". And a comparison is made between academics and professional services staff with interviewees commenting that: "Some of us are very into it and others just don't understand and it [is] just blocking their job, which it isn't, but they think it is"; "I think you'll have a higher compliance rate with us than you would with other teams around or other roles around campus". This demonstrates that there is compliance disparity between user groups across the HEI.

3) IT Expectations Finding 3: Users want to comply

Users want to comply with IT expectations because "it's within the framework of the organisation". A senior academic state their willingness to comply "Well, [..] we're in the business of [..] we're information security academics. So, I guess our day job is about- I mean in some sense, one part of our mission is to keep the world secure, to educate people about security practice". An interviewee comments, "so you know, [..] there's no clear guidance on how to behave with stuff like this and what to do if there's a problem."

Although, users are willing to comply with IT expectations, but there are some instances when they may not comply, as the following interviewee extract indicates: "I think we are very likely to comply, because I don't think they are too difficult to comply with. So again, I think there's this trade off, if they expect a lot from us, it will be more difficult to comply with, right? So not asking a lot, but asking something that is reasonable, is, [..] again makes it easier for us to comply". Further, interviewees say they will not comply under certain conditions: "if this is a restriction on my research"; things start to sound unreasonable and they start to become, an obstacle to our work, then the temptation not to comply increases"; "I think we'd only think it's excessive if it was actually hindering us being able to interact".

D. Moving Away from Phishing Exercises

The theme focuses on the observation that was made about how unproductive phishing exercises are and about the need to move away from it. The theme establishes the context for phishing exercises, if at all they are to be done. In which case it needs to be planned, people need to be informed and carried along, this has not been the case in HEIs.

1) Moving Away from Phishing Exercises Finding 1: Phishing exercises create more problems between the IT Team and users

Phishing exercises create problems of distrust and resentment between IT team and users. An interviewee says, "these kind of so-called realistic phishing exercise [..] will probably cause more problems than solving problems because it will cause some confusion, that can potentially even make the functionality fail". Another interviewee comments, "I'd find it a little bit, I guess in a way I'd feel it's a little bit violating that your own university is trying to phish you, even if it's to teach you a lesson, you know, it feels a bit off-putting". Phishing of staff creates anger as these interviewee extracts indicate: "I know some

colleagues who were very angry about it, particularly, they thought, they were insulted that they were being phished by the, especially the information security staff"…"but equally I think it annoys people as well".

2) Moving Away from Phishing Exercises Finding 2: Phishing exercises results used to blame others

There is the tendency that phishing exercises results could be used by the university to blame people [36]. This is the undertone of this extract "[..] for those that got caught, it would have been a bit of a wakeup call, I suspect, and it wasn't, and are probably feeling a bit stupid and being a bit cross about it, but actually if they think about it for 30 seconds, they should be quite glad that they clicked on something that was quite innocent and it was helping them raise awareness". Similarly, an interviewee raises a concern about "the risks with these phishing techniques are that they might be just used to blame users and that's, not ideal". In view of aforementioned arguments, some users feel it causes panic and advise that "it is not the way forward".

3) Moving Away from Phishing Exercises Finding 3: Phishing exercises opposed

Phishing exercises are opposed to. For instance, one interview states that there is "a lot of bad feeling from staff who felt that this is not a particular way to go". Due to the negative feelings from users, they have shown resistance to the implementation of phishing exercises.

E. Training, Reinforced Training and Awareness

Training is needed in universities by users and cyber security staff alike. This theme majors on user behavioural change through training and awareness, with a knock-on effect on security culture. The focus of the theme is on all users (including IT staff and students) and how to better equip them to secure information assets. It is through training and awareness that mindsets that influence unsafe user behaviour could be changed.

1) Training, Reinforced Training and Awareness Finding 1: Cyber security training is lacking

Our finding shows that cyber security training is lacking as an interviewee admits, "No. There's no such thing as far as I understand. There's no cyber security training for staff or students as far as I'm aware". Further, another interviewee states that there is "No cyber security training for staff or students". Interviewees recognised that it may be about signposting for the training: "But I've not been on anything [portal] that says, "this is cyber security, and you shall do it"; "there isn't any, what I would describe as dedicated on-boarding training around students for cyber security and institution". The lack of cyber security training could create vulnerabilities and awareness problems that cyber attacks may exploit.

F. Cyber Security Culture Measurement

Cyber security culture is hard to define, grasp and measure [16]. In view of this, it is the observable aspects of CSC that should be measured. These aspects of CSC are training over time, training uptake, incident reporting, cyber security climate, etc. This is an upcoming area of research that is currently being explored. The theme revolves around how to measure the observable aspects of CSC and its implementation across HEIs.

1) Culture Measurement Finding 1: Lack of knowledge about culture measurement

Interviewees feel that security culture is not measured in the HEIs, that it is difficult to measure, and that there is lack of understanding on how to measure it. For instance, interviewees commented that: "I don't think we measure culture, and I don't think most people know how to measure the culture"; "it's quite difficult to measure the culture".

VI. DISCUSSION AND RECOMMENDATIONS

A. Communication

The lack of systematic communication on cyber security between the IT team and users could be due to the absence of the needed training and communication skills among IT staff.

In some HEIs, restructuring of the cyber security and IT teams have led to under-resourced teams with reduced manpower. Hence, IT teams must prioritise and concentrate on technical solutions and approaches, the "traditional means" for defending universities' information assets. Focusing on technical solutions over the human aspect of cyber security could have resulted in the lack of interest in systematic communication with users. The restructuring within universities could also have been influenced by limited financial budget and insufficient cyber security investment, a challenge many Western HEIs face [37]. The same resource issue is a problem Malaysian HEIs experience, which delay the adaptation and implementation of security policies [38].

A reason for unclear communication could be the lack of understanding of what is to be communicated. For example, policies, training content, safe security behaviours or best practices. The communication problem is corroborated by the JISC survey on digital experience insight in UK HEIs [39]. The survey reports that 39% of students state that they were not informed by their institution how their personal data was stored or used. Also, it could be challenging for IT staff to translate technical information into simple layman's language for non-technical users to understand. Conversely, translating information on human aspects of security into technical solutions by IT staff is not an easy task as ENISA reports [40].

The collaboration problem between the IT team and academics could be caused by the lack of engagement in times past, which leaves no room for ideas to be shared and received. The IT team may also see the offer from academics as a way of monitoring their work. The culture of 'us versus them' could also have influenced the IT teams not embracing the offer of help from academics.

 ISBN: 978-1-61208-893-8

Some of the different perspectives provided by academics with information security background is that of their willingness to offer their expertise to assist the IT team and improve the cyber security posture in the HEI. Some feel that it is through the sharing of experiences and best practices that HEIs could be better prepared for security incidents.

Furthermore, issues of distrust caused by the implementation of phishing exercises in HEIs could have strained the relationship between academic and IT staff, thus making collaboration less likely. It is also likely that the IT team and the university have been busy 'firefighting' and have been overwhelmed by the 'catch-up game' with cyber-attacks; as a result, they may not have time for engagement with users.

The impersonal communication from the IT team may be something that IT does not have control over. For instance, not putting an IT staff member's name on a service desk email could have been a senior management decision to increase request response rates. However, interviewees do not comment negatively on IT team's efficiency or excellence.

In view of our findings, a recommendation would be that senior management invest more in training and development for IT teams with specific focus on informing, engaging and persuading.

B. Policies and Frameworks for Guiding Cyber Security Behaviour

The lack of enough policies/framework could have been caused by lack of clear strategy needed to influence these written rules. Also, senior management may not have the expertise required to create polices/frameworks. Furthermore, other priorities could have taken the place of policy creation. The implication of these is that users engage in actions, activities, and habits which they perceive to be right but that may turn out to be detrimental to the security of HEIs assets.

Unclear and insufficient policies will lead to limited knowledge, understanding and awareness among users, as the available policies may not cover some security aspects which need protection. This creates some compliance gaps as some security expectations will not be known and cannot be followed. It then becomes difficult for users to see their role as critical in sustaining the security of their university. Users' attitude could also be affected negatively because they are not aware of frameworks that could guide them. Hence, they may see security as the IT team's problem and may not bother about incident reporting.

At times, policy creation responsibility of senior management is delegated to other staff members, but there is no guarantee that the staff members have the necessary skills to execute the duties. The study [41] shows where duties intended for senior leaders are delegated, outcomes are suboptimal.

It is possible that policies are not in place because they are not prioritised by senior management. Maybe regulatory compliance like GDPR is prioritised over security policies, to avoid reputational damage and fines. Prioritisation issues in policies could be caused by lack of understanding about the risks and threats HEIs face. Also, there is the lack of understanding on how to conduct cyber security measurement. It then becomes difficult for senior management to make decisions about policies, prioritise the allocation of significant but limited resources to address increasing vulnerabilities and cyber attacks.

We observe that HEIs' cyber security strategy is unclear and not fully operational. This means that strategy could not influence policies, resulting in a lack of clarity and prioritisation in policies. Communicating policies will be hindered further because of the problems we identify in the key theme, communication.

To address the aforementioned problems, a recommendation would be that senior management prioritise the creation of a cyber security strategy, around which security policies could be built. This could be a starting point which expands to various cyber security areas. HEI leaders should engage academics' expertise within their institutions, to assist in the creation of policies, something that we did not observe, and which caused additional friction. Policies should specify the expected security behaviours of users. There should also be a way testing users' understanding of policies as communication is not effective until recipients understand the information being conveyed. Additionality, training on using quantitative approach for CSC measurement should be provided to the relevant HEI teams.

C. IT Expectations

IT Expectations Finding 1 indicates that IT expectations are not well defined. The possible cause of this could be that those responsible for defining IT expectations lacks the required understanding. This is similar to the lack of understanding of security culture that results in CSC being ill-defined [16]. Other possible causes of unclear IT expectations could be the lack of cyber security strategy, resource limitations, and time pressures on the IT staff.

The lack of strategic direction and expectations that users see may result in them not having trust in any of the IT expectations that they are advised about. The act of senior cyber security academics approaching IT teams to offer help may indicate that serious problems exit in the IT teams and within its processes.

Also, there could be a knowledge gap between IT staff and academics which might have an influence on the users' attitudes to learning about cyber security. This attitude could have resulted in compliance disparity that we observe among the user groups. For example, we saw reported a higher security compliance rate among administrative staff, who are better informed on security-related processes, in comparison to academics.

 ISBN: 978-1-61208-893-8

Users indicate they will comply with IT expectations if they know what these expectations are. Their willingness to comply is a positive attitude towards security. From our study, we observe that users, ranging from academics to students see the need for compliance and understand its benefits. This compliance readiness is what the HEIs could work with and use for 'nudging' users towards cultivating certain security behaviours in the university [42]. Small changes could be introduced in the design of solutions, where decisions need to be made. For example, nudges could be used where a user needs to decide whether or not to report a security incident. In this way, the user is encouraged to adopt the desired behaviour leading to an incident reporting. While a one-size-fits-all nudge approach may produce a useful outcome, personalised nudges could be more effective, although personalised nudges have been seen as threat to user autonomy [43].

However, compliance even when expectations are known does not always happen. Our study shows that users will resist unrealistic expectations, as common sense implies. It is therefore important for IT staff in HEIs to engage and communicate with users, particularly where expectations could be perceived as borderline/unrealistic. This might enhance user understanding and, thus, compliance.

Extant literature confirms our finding of distrust, and it states that phishing exercises create more problems than solve them [36]. The literature points out the reasons why an organisation should not phish staff as it creates distress, and even distrust between users and security, as some of the interviewees in our research explain.

Given the aforementioned challenges, we recommend that IT expectations are reviewed by a multi-disciplinary team.

D. Moving Away from Phishing Exercises

To promote collaboration and engagement between the IT team and users, the implementation of phishing exercises is to be avoided. HEIs represent freedom of expression and openness. Utilising an approach which causes distrust stifles relationship-building and collaboration. Using the outcomes of phishing exercises to blame users could create an environment that is void of transparency and openness. There is a tendency that blaming users could stop them from reporting security incidents or near misses when they occur. Therefore, an opportunity for the IT team to address a vulnerability could be left to a cyber attack to exploit.

It seems that resistance to phishing exercises come from almost all users, except for senior management that might have authorised them in the first place. Even if phishing exercises were to be used, the time needed to think through, and administer non-repetitive innovative exercises by HEIs IT teams may not be available.

Some academics feel phishing exercise could be used to understand the current cyber security state of the university. For example, the level of preparedness of users, which individual needs to be upskilled. Increasing security knowledge in HEIs is seen as important but there is a feeling that there is more to security knowledge that sending out phishing emails and making personnel attend mandatory training.

In line with a senior security staff interviewee, we argue that the implementation of phishing exercises approach should be avoided. We recommend that HEIs senior management investigate the problems caused by implementing phishing exercises in their HEIs from users' perspective. A clear picture could only be seen if senior management examine users' attitude toward security issues, their security behaviours and how critical they now consider their responsibilities to be in securing HEIs information assets, after they have been phished. This is likely to change senior management's opinion towards implementing phishing exercises in their HEIs.

E. Training, Reinforced Training and Awareness

The lack of enough cyber security training in HEIs could be because of limited financial resources in HEIs [38]. Also, prioritisation issues identified in policies and ill-defined IT expectations may mean that the most pressing security need is not identified and as a result could not be addressed by training. For example, our study did not observe social engineering training as a matter of priority in HEIs.

The implication of insufficient training is that users engage in unsafe security behaviours that could compromise security. Without adequate training, users are not aware, are uninformed, and are not equipped to deal with current security issues. This could make HEIs and other users susceptible to cyber attacks.

We observe that a link exists between training, communication, and policies. Training can be used to communicate policies to users, thus bringing awareness, understanding, and influencing cyber security culture across the HEIs. Training approach and training content are also important. When training users, storytelling and other approaches that have been found to promote engagement and knowledge transfer should be considered.

As security compliance is influenced by training, it is important for cyber security training to be taken seriously by HEI senior management. Furthermore, there are cloud computing challenges with distant learning following the changes introduced by Covid-19 lockdown which affects education delivery [44].

We recommend that senior management prioritise and invest in trainings, including offering training that focuses on social engineering and other human aspects of security.

F. CSC Measurement

An understanding of how to measure CSC and its implementation across institutions is needed. From our analysis, we found that people/universities do not know how to measure CSC. Also, the scales and the matrices that have been promoted by standard bodies such as International Organisation for Standardisation (OSI), National Institute of Standards and Technology (NIST) and Open Web

Application Security Project (OWASP), does not consider the complexity of cyber security, changing technology and human agents [3]. Hubbard and Seiersen [3] argue that compliance with standards and regulations does not improve cyber security risk management and the metrics for assessing the risks are flawed.

If the approach of assessing cyber threats and measuring security risk and culture is flawed or not known, then the true state of security in HEIs may not be determined. This makes informed decisions about resource allocation and other security investments a challenge for HEI senior management. Without the ability for assessing the current state of security through training uptake, incident reporting and behaviour change, we cannot demonstrate that progress has been made in terms of CSC in HEIs.

We recommend that HEIs consider ways of conducting CSC measurement.

VII. CONCLUSION AND FUTURE WORK

Communication is the central theme that must be fully embraced and continuously utilised if CSC is to be developed in HEIs. Communication with its approaches is significant because without it, all the other themes that we identify in this study will not be impactful in HEIs. Thus, we establish that communication is interwoven with the themes – policies and frameworks, IT expectations, moving away from phishing exercise, training, reinforced training and awareness, and CSC measurement. These themes are the factors that influences personnel and students' view of CSC in HEIs.

Currently, the approach of communication in the HEIs we examined needs to change. This includes communication between the IT team and users, as well communication from senior management to HEI staff. While there is information flow from the IT teams to users, we observe that dialogue is lacking. Hence, a new approach is needed that promotes engagement and collaboration.

Training, reinforced training and awareness are necessary to ensure that security information communicated through policies, frameworks and programmes are always at the fingertips and on the minds of users. Hence, training and awareness require an effective communication strategy so that its delivery could make maximum impact and change people's mindsets towards cyber security. In view of this, no-one should be exempted from training, irrespective of their status or hierarchy within the institutions.

There must be a conscious effort and drive from senior management team to create multi-disciplinary team of experts who will champion the promotion of CSC in HEIs and challenge the reactive attitude of "always being in the catch-up game with cyber attacks". The multi-disciplinary team could also be involved in co-creating policies by involving other users and fostering engagement. This approach will be a useful one for replacing phishing exercises which we have proved to be problematic, ineffective and have also been strongly opposed by academics, students, and other users.

The expertise of academics in HEIs have not been fully utilised in the quest to defend the institutions from cyber attacks. We recommend that senior management members kick-start an initiative to engage academics and seek ways of using their expertise, experience, and their innovative approach for defending the information assets of the HEIs. Any solutions that come out of the initiative could be integrated into the university training and awareness programmes and could also be shared with other sectors.

In sum, the implementation of a communication strategy, engagement and collaborative effort will be valuable in developing a cyber security culture and by so doing securing information assets of HEIs and reducing security breaches caused by human error.

There are a few limitations of the study. As in all qualitative analysis, researchers bias could be a concern. To avoid self-reporting bias [45] and maximise the value of our approach, leading questions were avoided. We used open-ended questions, allowing the interviewees to give detailed answers, using their own words. Further, more personnel could have been interviewed in our study. The barrier to this, was the Covid-19 lockdown which affected the response we received from the HEI personnel we contacted.

Our research shows that there is limited or no measurement of CSC in the HEIs that we examined. Hence, future research could investigate how CSC could be measured in different HEIs. Also, research can explore how cyber security training needs of different users in various departments could be identified. Appropriate training can then be geared towards an individual user instead of applying a one-size-fits-all approach. Another aspect that could be researched is HEIs' response to embracing technological change following the disruption introduced by the Covid-19 pandemic.

REFERENCES

[1] C. Kyriazopoulou, "Smart city technologies and architectures: A literature review", in 2015 International Conference on Smart Cities and Green ICT Systems (SMARTGREENS). 2015 International Conference on Smart Cities and Green ICT Systems (SMARTGREENS), 2015, pp. 1–12.

[2] A. A. Rahman, U. Z. A. Hamid, and T. A. Chin, "Emerging Technologies with Disruptive Effects: A Review", PERINTIS eJournal 7(2), p. 19, 2017.

[3] D.W. Hubbard and R. Seiersen, "*How to Measure Anything in Cybersecurity Risk"*. Hoboken, NJ, USA: John Wiley & Sons, Inc 2016. doi: 10.1002/9781119162315.

[4] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N.A. Ghani, and T. Herawan. "Information security conscious care behaviour formation in organizations", *Computers & Security*, 53, pp. 65–78, 2015. Doi: 10.1016/j.cose.2015.05.012G.

[5] J. Chapman. "How safe is your data? Cyber-security in higher education". HEPI Policy Note, vol. 12, Apr. 2019.

[6] PwC [online] Available at: <https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf> [Accessed: September 2021].

[7] IBM, “IBM 2015 Cyber-Security-Intelligence-Index”. Available at: https://essextec.com/wp-content/uploads/2015/09/IBM-2015-Cyber-Security-Intelligence-Index_FULL-REPORT.pdf (Accessed: September 2021).

[8] K. Huang and K. Pearlson, “For What Technology Can’t Fix: Building a Model of Organizational Cybersecurity Culture,” Proc. of the 52nd Hawaii International Conference on System Sciences, Jan. 2019, pp. 6398-6407.

[9] A. Ahmad, K. C. Desouza, S. B. Maynard, H. Naseer, and R. L. Baskerville, 2020. "How Integration of Cyber Security Management and Incident Response Enables Organizational Learning," Journal of the Association for Information Science and Technology, vol. 71:8, 2020, pp. 939-953.

[10] A. Wiley, A. McCormac, and D. Calic, “More than the Individual: Examining the Relationship Between Culture and Information Security Awareness,” Computers & Security, vol. 88, Jan. 2020, doi: 10.1016/j.cose.2019.101640.

[11] A. Georgiadou, S. Mouzakitis, and K. Bounas, D. Askounis, “A Cyber-Security Culture Framework for Assessing Organization Readiness”, *Journal of Computer Information Systems*, pp. 1–11, 2020. Doi: 10.1080/08874417.2020.1845583.

[12] B. Von Solms, “Information Security — The Third Wave?”, *Computers & Security*, vol. 19(7), pp. 615–620, Nov. 2000. Doi: 10.1016/S0167-4048(00)07021-8.

[13] A. Da Veiga and J. H. P. Eloff, “A framework and assessment instrument for information security culture”, *Computers & Security*, vol. 29(2), pp. 196–207, Mar. 2010. Doi: 10.1016/j.cose.2009.09.002.

[14] R. Reid and J. Van Niekerk, “From Information Security to Cyber Security Cultures Organizations to Societies”. Information Security South Africa (ISSA), vol. 38, pp. 97-102, 2014.

[15] L.J. Hadlington, “Employees attitudes towards cyber security and risky online behaviours: an empirical assessment in the United Kingdom”. International Journal of Cyber Criminology. vol. 12 (1), pp. 269–81, Jan-Jun. 2018.

[16] N. Gcaza and R. Solms, “Cybersecurity Culture: An Ill-Defined Problem”, IFIP World Conference on Information Security Education (WISE 2017) pp. 98-109, 2017. Doi: 10.1007/978-3-319-58553-6_9.

[17] Jisc.ac.uk. [online] Available at: <https://www.jisc.ac.uk/sites/default/files/dei-2020-student-survey-question-by-question-analysis.pdf> [Accessed: September 2021].

[18] K. Roer, et al. “Measure to Improve, Security Culture Report 2020”. [online] Available at: <https://www.knowbe4.com/hubfs/Security-Culture-Report.pdf> [Accessed: September 2021].

[19] Ico.org.uk. *The University of Greenwich fined £120,000 by Information Commissioner for “serious” security breach*. [online] Available at: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/05/the-university-of-greenwich-fined-120-000-by-information-commissioner-for-serious-security-breach/> [Accessed: September 2021].

[20] D. Sanderson, “*Edinburgh University hit by freshers’ week cyberattack”*. [online] Thetimes.co.uk. Available at: <https://www.thetimes.co.uk/article/edinburgh-university-hit-by-freshers-week-cyberattack-0m2xzl0p8> [Accessed: September 2021].

[21] J. F. Van Niekerk and R. Von Solms, “Information Security Culture: A Management Perspective”. Computers & Security, Vol. 29 (4), pp. 476-486, 2010.

[22] S. H. Bakry “Development of e-government: A STOPE view”, International Journal of Network Management, vol.14 (5) pp. 339-350, 2004.

[23] A. Alhogail and A. Mirza, “Information Security Culture: A Definition and A Literature Review,” World Congress on Computer Applications and Information Systems, WCCAIS, pp. 1-7, Jan. 2014. doi: 10.1109/WCCAIS.2014.6916579.

[24] A. Da Veiga and N. Martins, “Information security culture: A comparative analysis of four assessments”. Proceedings of the 8th European Conference on IS Management and Evaluation, 2014, pp 49-57.

[25] M. Alnatheer, “Information Security Culture Critical Success Factors”. 12th International Conference on Information Technology - New Generations, 2015, pp. 731-735.

[26] M. Bada, A. Sasse, and J.R.C Nurse, “Cyber security awareness campaigns: Why do they fail to change behaviour?” International Conference on Cyber Security for Sustainable Society, 2015.

[27] M. Ioannou, E. Stavrou, and M. Bada, "Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination," 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 2019, pp. 1-4, doi: 10.1109/CyberSecPODS.2019.8885240.

[28] R. Knight and J. R. C. Nurse, (2020). A framework for effective corporate communication after cyber security incidents. Computers & Security, vol. 99, Sep. 2020. https://doi.org/10.1016/j.cose.2020.102036

[29] A. Da Veiga, “An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture”. Information & Computer Security, vol. 26(5), pp. 584-612, Jun. 2018 https://doi.org/10.1108/ICS-08-2017-0056

[30] M. C. Van’t Wout, “Develop and Maintain a Cybersecurity Organisational culture”. ICCWS 2019 14th International Conference on Cyber Warfare and Security, Academic Conferences and Publishing Limited, pp. 457-466, Feb. 2019.

[31] C.F. Cannell, P.V. Miller, and L. Oksenberg, “Research on Interviewing Techniques”. Sociological Methodology, vol. 12, pp. 389–437, 1981.

[32] C. Erlingsson and P. Brysiewicz, “A hands-on guide to doing content analysis”, *African Journal of Emergency Medicine*, vol. 7(3), pp. 93–99, 2017. doi: 10.1016/j.afjem.2017.08.001.

[33] H.F. Hsieh and S.E. Shannon, “Three Approaches to Qualitative Content Analysis”, Qualitative Health Research, vol. 15(9), pp. 1277–1288, 2005. doi: 10.1177/1049732305276687.

[34] S. Elo and H. Kyngäs, “The qualitative content analysis process”, Journal of Advanced Nursing, vol. 62(1), pp. 107–115, 2008. doi: 10.1111/j.1365-2648.2007.04569.x.

[35] A. Ertan, G. Crossland, C. Heath, D. Denny, and R. Jensen, “Cyber security behaviour in organisations” 2020. arXiv preprint arXiv:2004.11768.

[36] Ncsc.gov.uk. “*The Trouble with Phishing”* 2018. [online] Available at: <https://www.ncsc.gov.uk/blog-post/trouble-phishing> [Accessed: September 2021].

[37] J. Ulven and G. Wangen, “A Systematic Review of Cybersecurity Risks in Higher Education”. Future Internet, 2021, 13(2), 39, https://doi.org/ 10.3390/fi13020039

[38] W. Ismail and A. Widyarto, “A Formulation and development process of information security policy in higher education”. Proc. of the 1st International Conference on Engineering Technology and Applied Sciences, Afyonkarahisar, Turkey, pp. 21–22, April 2016.

[39] Repository.jisc.ac.uk. 2018. [online] Available at: <https://repository.jisc.ac.uk/6967/1/Digital_experience_insights_survey_2018.pdf> [Accessed: September 2021].

[40] Enisa. 2018. [online] Available at: <https://www.enisa.europa.eu/publications/cybersecurity-

culture-guidelines-behavioural-aspects-of-cybersecurity> [Accessed: September 2021].

[41] G. Gearhart and M. Miller “Higher Education’s Cyber Security: Leadership Issues, Challenges, and the Future”, Journal of New Trends in Education, vol. 10 (2), pp. 11–18, 2019.

[42] R.H. Thaler and C.R. Sunstein. Nudge: Improving decisions about health, wealth, and happiness. New Haven: Yale University Press, 2008.

[43] N. E. Diaz Ferreyra, E. Aïmeur, H. Hage, M. Heisel, and C. van Hoogstraten, “Persuasion Meets AI: Ethical Considerations for the Design of Social Engineering Countermeasures”, Proc. of the 12th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management, pp. 204-211, Nov. 2020. Doi: 10.5220/0010142402040211

[44] S. Bhagat and D.J. Kim, “Higher education amidst COVID-19: Challenges and silver lining”. Information. Systems. Management, 2020, vol. 37(4), pp. 366–371. https://doi.org/10.1080/10580530.2020.1824040

[45] V. Jupp, The SAGE Dictionary of Social Research Methods. SAGE Publications, London Thousand Oaks, California, 2006.