Cyber-risk in Healthcare: Exploring Facilitators and Barriers to Secure Behaviour

Lynne Coventry[1[0000-0002-6600-8414]], Dawn Branley-Bell[1[0000-0003-0105-5495]] , Elizabeth Sillence[1[0000-0003-1085-7115]] Sabina Magalini[2 [0000-0002-4056-1115]], Pasquale Mari[2 [0000-0002-1136-9722]], Aimilia Magkanaraki[3 [0000-0002-9025-8456]], and Kalliopi Anastasopoulou[3[0000-0002-8782-8307]]

[1] Northumbria University, Newcastle upon Tyne NE1 8ST, UK
lynne.coventry@northumbria.ac.uk
dawn.branley-bell@northumbria.ac.uk
elizabeth.sillence@northumbria.ac.uk

[2] Fondazione Policlinico Universitario Agostino Gemelli, Rome, Italy
Sabina.Magalini@unicatt.it
Pasquale.mari3@gmail.com

[3] 7th HealthCare Region of Crete, 3rd klm of National Road Heraklion-Moires, 71500, Heraklion, Crete, Greece
amagkanaraki@hc-crete.gr
kanastasopoulou@hc-crete.gr

Abstract. There are increasing concerns relating to cybersecurity of healthcare data and medical devices. Cybersecurity in this sector is particularly important given the criticality of healthcare systems, the impacts of a breach or cyberattack (including in the worst instance, potential physical harm to patients) and the value of healthcare data to criminals. Technology design is important for cybersecurity, but it is also necessary to understand the insecure behaviours prevalent within healthcare. It is vital to identify the drivers behind these behaviours, i.e., why staff may engage in insecure behaviour including their goals and motivations and/or perceived barriers preventing secure behaviour. To achieve this, in-depth interviews with 50 staff were conducted at three healthcare sites, across three countries (Ireland, Italy and Greece). A range of seven insecure behaviours were reported: Poor computer and user account security; Unsafe e-mail use; Use of USBs and personal devices; Remote access and home working; Lack of encryption, backups and updates; Use of connected medical devices; and poor physical security. Thematic analysis revealed four key facilitators of insecure behaviour: Lack of awareness and experience, Shadow working processes, Behaviour prioritisation and Environmental appropriateness. The findings suggest three key barriers to security: i) Security perceived as a barrier to productivity and/or patient care; ii) Poor awareness of consequences of behaviour; and iii) a lack of policies and reinforcement of secure behaviour. Implications for future research are presented.

Keywords: Cybersecurity; Health; Healthcare; Cyberthreat; Behaviour Change

1 Introduction

Cybersecurity in healthcare is of increasing concern. New technological interventions continue to improve the treatment of a wide range of medical issues, and undoubtedly, healthcare technology has potential to save, and enhance, human life [1–3]. Many hospitals now operate using a complex interconnected network of IT systems and devices. This includes connected health devices and administration systems storing electronic health patient records (EHRs). Hospitals and clinics also rely upon remote working and/or the transfer of test results and other sensitive data via electronic channels [4]. Unfortunately, an increase in new technology and interconnectivity also introduces new security vulnerabilities and challenges [5, 6]. This is not purely a technical problem, but a complex sociotechnical one that will only be solved by understanding ways in which technology and humans can interact to create the strongest defences; as well as the way that this interaction can create vulnerabilities.

Healthcare is an attractive target for cybercrime for two fundamental reasons: it is a rich source of valuable data [4] and its defenses are weak [6]. The mass media highlights that vulnerabilities within healthcare are being exploited [7, 8], and the sector urgently needs to increase its resilience against cyberattacks and breaches [6, 8]. Breaches can reduce patient trust, cripple health systems and threaten human life [9]. The WannaCry attack in 2017 is a key example of the type of consequences that cyberattacks can have within the healthcare sector [10]. WannaCry was a ransomware attack which affected computers in more than 100 countries. The National Health Service (NHS) England was amongst those affected. with 80 (34%) NHS trusts, 603 primary care organisations and 595 GP practices infected by the ransomware. This resulted in the cancellation of over 19,000 patient appointments, and a substantial financial cost to the NHS [11]. Around the world, ransomware attacks are still being experienced, disrupting services, and even forcing some practitioners to quit the healthcare sector [12]

Although technological protection such as strong firewalls and antivirus can go some way towards protecting against cyberthreat; strong cybersecurity also relies upon secure staff behaviour, which has largely been ignored [6]. Cybersecurity is not just a technical problem, but a complex sociotechnical problem [13]. Staff behaviour has been shown to be one of the major contributors to cybersecurity vulnerability [4] and humans have often been described as cybersecurity's 'weakest link' [14]. However, it is important to recognise that staff can also be one of the strongest links in cybersecurity, when secure employee behaviour acts – in effect – as a 'human firewall' [6].

Whilst in some instances, staff misbehaviour is deliberate, i.e., deliberate insider threat. A significant proportion of cyberattacks and breaches are unintentional consequences of staff behaviours that introduce vulnerability without malicious intent [4]. Healthcare represents a unique environment, one where staff prioritise effective and efficient patient care. Understandably, cybersecurity may not be the primary focus during their day-to-day working lives. Staff working within this sector also report being overworked, fatigued and stressed [15–18]. This creates psychosocial risks for cybersecurity [19]. It is important that research identifies key vulnerabilities in staff behaviour and investigates how to address these in a manner that does not burden staff and/or

negatively impact upon patient care. In order to do this, it is necessary to identify the driving factors behind staffs' insecure behaviour, for example is this behaviour driven by a need to save time? Due to a lack of awareness? Or some other factor(s)? Previous research shows a range of factors which can influence secure or insecure behaviour, including for example self-efficacy, attitudes, external influences, coping and threat evaluation [20]. Many insecure behaviours have been found to be instrumental, reasoned and conducted as a means to an end, e.g., to save time [4]. Therefore, effective interventions can only be designed following the identification of drivers behind insecure behaviour [4]. This study addresses this gap in the current literature through a series of in-depth focus groups and interviews with healthcare staff across three sites, and three countries (Ireland, Italy and Greece); enabling the exploration and identification of key barriers to cybersecurity in the healthcare environment.

To summarise the main contributions of this study are:

- Identification of insecure behaviour(s) by healthcare staff
- Identification of the key factors facilitating insecure behaviour(s) and/or providing barriers to more secure behaviour
- Preliminary discussion of the implications of these findings for the design of interventions and the role of HCI in facilitating secure behaviour.

2 Methodology

Three focus group sessions took place across three sites: Gemelli hospital in Rome, the 7th Health Region of Crete, and the HSE SSW Hospital Group, Ireland. These sessions were conducted face-to-face at the hospital location or remotely via Skype. Each session lasted between 45-60 minutes, and included between 2-9 staff members. A total of 50 staff took part. A range of healthcare staff were included from administration staff, doctors, nurses, IT staff, etc. (Table 1).

Table 1. Job Roles

Location	Job Role
Gemelli Hospital, Rome	Lab Technicians
	Administration Staff
	IT Team
7^{th} Health Region of Crete (7HRC)	IT Teams across 2 different hospitals
	Biomedical Engineers
	Health Centre Staff (nurses, GPs, health workers)
	Managers
The HSE SSW Hospital Group, Ireland	Lab Technicians
	Administration Staff
	Medical Consultants
	Finance Staff

	Emergency staff including paramedics and ambulance staff
	Nurses
	Doctors

During the focus group, the facilitators asked opened ended questions focusing upon the following areas:

- Awareness of any previous incidents at the hospital they would describe as cyber-related
- Type of cybersecurity risks that staff felt were of most concern within the hospital
- The type of data and technology that staff interact with on a daily basis and the perceived security of this technology
- Security of staff behaviour and any risky behaviours that they were aware of
- General awareness of potential cyber-risk and vulnerability to attack.

For those interviewees that could not attend the focus groups (for example, due to unforeseen patient emergencies), we collected additional survey-based responses to these questions. The results were analysed using thematic analysis [21] to identify key themes. Ethical approval was granted by Northumbria University ethics committee before commencing.

3 Results

This section describes the five themes that developed in the analysis. The first details the type of insecure cybersecurity behaviours occurring across the healthcare sites. The remaining four themes explain key facilitators underpinning these behaviours: Lack of awareness and experience; Shadow working processes; Behaviour prioritization and Environmental appropriateness.

3.1 Insecure Cybersecurity Behaviours

Within this theme, seven types of insecure cybersecurity behaviours were identified that would pose a risk to healthcare institutions: *Poor computer and user account security; Unsafe e-mail use; Use of USBs and personal devices; Remote access and home working; Lack of encryption, backups and updates; Use of connected medical devices; and poor physical security.* These were identified as risk behaviours as they have been linked to increased cybersecurity risk in the literature [22].

Poor Computer and User Account Security

Concerns around the security of login credentials and computer access were prevalent across all three sites. Two major concerns were noted: *Open workstations* within the hospital and *poor password security.*

Many participants reported that computers within the healthcare environment are often used/shared by many different users. To save time logging in and out of their individual accounts, staff report leaving workstations logged into a single staff user account. Because of this, it is common to find *open workstations* throughout the hospital. Users were particularly likely to leave a computer logged into a single staff members account within the labs – where it was perceived that only known individuals would have physical access to the computer. This suggests that trust amongst colleagues plays a role in this behaviour.

Password security was a subject over which both the medical staff and the IT staff expressed frustration. IT staff described *poor password security* as a "single point of [security] failure". We identified three key areas of concern: *repetition of passwords, writing passwords down,* and *use of automatic login/remember me* options on the workstations. Within the hospital, systems are in place that require employees to change their work passwords periodically (usually around every 2-3 months). The system does not allow staff to use the previous 2-3 passwords, however some staff report simply using the same 3-4 passwords on a rotating cycle to get around this, and to help them remember their passwords. Staff report frustration that it is "not possible to remember 20 different passwords" – so users use the same passwords across multiple systems as often as possible (often the same password they use for personal computer and internet use). As aforementioned, junior and admin staff often use senior staff login credentials; due to this they tend to be the first to receive the notice that the current password is about to expire. Consequently, junior and admin staff often change doctors and directors' passwords. This could result in passwords that may be difficult for the senior staff to remember (due to a lack of personal salience).

Systems generally generate specific password requirements (e.g., the password must be more than a specified number of letters, contain a number or symbol, etc.). This is designed to support secure password choices; however, staff report that these rules vary across the different platforms that they use and this can lead to frustration. All of the factors (number of passwords required, regular need to update passwords, staff member changing others' passwords, and differing password requirements) can contribute to difficulty in password memorability. Consequently, many staff report that passwords are written down - often on sticky labels attached to computer monitors, visible by everyone. Many computer systems also ask staff if they would like the computer to automatically remember their login credentials, e.g., by ticking "remember me" or "save password". This is not a recommended security behaviour, particularly on shared devices, however, staff often accept this option to save time and forgotten passwords. Staff do not generally use a secure password manager to remember passwords (e.g., KeyPass), with the exception of some IT staff. While 'remember me' may improve usability it has an unintended consequence for security.

Phishing

Staff use e-mail on a daily basis, and we identified concerns around dealing with *phishing emails* which may lead to stolen credentials or introduction of malware into the system. Staff reported *phishing e*-mails as a regular, ever increasing occurrence, and IT staff described it as a key cause for concern. Although spam filters are in place, these

often fail to keep up with ever-evolving phishing approaches and do not always correctly identify e-mails as spam. Conversely, important e-mails can also be incorrectly diverted to the spam folder – providing a potential barrier to staff productivity. Furthermore, reliance upon spam filters could provide staff with a false sense of security and the inaccurate assumption that those e-mails which reach their inbox must be 'safe'. Therefore, training and staff awareness is important.

At *some* of the hospitals, IT staff send regular internal e-mails warning staff not to open attachments. However, staff perceive this advice as unfeasible as they often need to open email attachments to do their job. Medical reports and assessments are often sent as email attachments by patients, patients' friends/family, and by other clinics and medical facilities (e.g., clinics across the region). Due to staff not knowing who will be e-mailing the document(s), they cannot rely upon recognising the e-mail address to identify if this is a genuine/safe e-mail. Instead, staff rely upon recognising (or searching for) the patient's name in the email subject box. This introduces significant vulnerability to exploitation. In addition to being unfeasible, advice from IT to not open attachments was perceived as contradictory, as genuine internal e-mails from IT and management often include links or attachments.

Use of USBs and Personal Devices

Staff reported regular use of USB sticks to save and transfer data at work. USBs are typically their own personal devices, not supplied by their employer nor used exclusively for work. All levels of staff reported using USBs, including junior and admin (e.g., to pass files to senior staff and directors), doctors, nurses, hospital residents (i.e., students) and IT staff. Perhaps even more concerning, external visitors and patients often bring their records on USB sticks to the hospital (e.g., reports from other clinics). These USBs are plugged straight into the hospital workstations without any prior safety procedures. These workstations are connected to the hospital network and not isolated machines. Sites differed in regards to whether an antivirus automatically scans USB devices when they are inserted into a computer; however even if this is activated it may not stop malware spreading. To try to minimise risk, some IT teams have closed the USB ports on specific workstations (e.g., computers within the radiology department) but this is not generally the norm across most machines.

Staff generally perceived no danger related to USB use, with the exception of the IT and technical teams who expressed concern but also regarded USB usage as necessary, and therefore unavoidable. Indeed, in some roles, USBs actually form part of the compulsory method for staff to confirm their identity by electronic signature.

In addition to USB sticks, staff bring other *personal devices* to work – such as laptops and smartphones (with many staff accessing work e-mail via their personal smartphone). Most staff reported that personal devices are only permitted to connect to the free public WiFi and not to the main hospital network. However, IT and technical staff described struggling to monitor and prevent staff from plugging their devices directly into the hospital network using Ethernet cables. This can be prevented by having ports paired with devices, however this is limiting when equipment is being regularly moved around the environment. In some limited circumstances, personal laptops can be connected to the hospital network with prior permission from IT. For those sites in

remote, rural areas or small practices, it is more common for staff members to use their own devices for work. In these circumstances there are not always restrictions on connecting these devices to the hospital systems. Lost or stolen devices pose a significant security concern, as IT do not install software to enable them to remotely wipe the device.

For some IT staff, the lack of a clear policy against bringing your own device to work is seen as a big problem. Unfortunately, any changes would have to be enforced by the governance board, who were generally described as lacking a "security mindset" and being reactive rather than proactive (i.e., waiting until something happens before acting rather than putting preventative measures in place).

Lack of Encryption, Backups and Updates

Alarmingly, no staff reported regularly encrypting data before transmitting it within - or particularly outside - of the hospital. This means that data being shared (and accessed on personal devices) represents an even greater vulnerability. Staff reported never being instructed – or taught – to encrypt files. A minority of the sites require staff to use SSL to send e-mails, and some departments (e.g., accounting) use digital signatures to exchange files, but this was in the minority.

Staff demonstrated a significant lack of awareness in relation to data backups, with most simply 'assuming' that backups took place automatically. Staff perceived backups as something that would be managed by IT or the department head – but they were not sure whether this was actually the case. In most cases this is correct, although staff should be made more aware what is and is not backed up from different devices. For instance, staff described how one senior manager's workstation could not be re-established after a ransomware attack as the manager had switched off the automatic backup software. Staff also reported a reluctance to install software updates on the workstations as they perceived these as problematic, e.g., "every update breaks one of the systems". Installation problems can result in time away from their job to solve the problem – often involving liaising with IT and/or external businesses responsible for the software or system. Therefore, although systems often alert staff when updates are required, these alerts are often dismissed by repeated use of the "remind me later" button. Additionally, staff often do not have time to shut down the system for upgrades, for example transplant personnel work 24/7 and do not perceive there to be a suitable time to shut down the workstations for updating.

Use of Connected Medical Devices

Some sites use a range of *connected medical devices* (i.e., devices connected to the internet) such as monographs, CT scanners, and MRI scanners. In general, staff perceived connected devices to be introducing new challenges and threats – that many did not feel prepared nor trained for.

For some of these devices, remote access is not possible – i.e., these cannot be controlled or accessed from outside of the hospital. This is typically achieved by the devices being on a separate internal network. However, for other devices, remote access is required by the device suppliers (e.g., to adjust device settings). This again raises

security issues. These issues can be complex to address as some responsibility for connected medical devices lies with the biomedical engineers, rather than IT – and IT staff describe the biomedical engineers as being "focused upon usability rather than security". IT staff also described the software used for medical devices as typically outdated and unsupported. This is concerning as it makes updating and patching impossible.

Poor Physical Security

In addition to more traditional cybersecurity risks, insecure physical access to healthcare facilities was also a concern for some sites. Facilities were often reported as being easy to enter with a lack of substantial physical barriers to prevent unauthorised access. Staff described unauthorised people frequently entering 'staff only' areas. This is particularly problematic in large hospitals where staff are unable to identify or recognise all of their colleagues. Furthermore, although offices may be locked, there are certain areas such as nurses and doctors' workstations which are always accessible. Security cameras have been installed in some locations to improve security, but the lack of additional physical security measures remains an issue.

3.2 Lack of Awareness and Experience

This theme explores participants lack of personal awareness of cyberattacks in their workplace and the potential consequences of their actions.

While awareness of cyberthreats and data breaches in general is high, previous experience of cyber breaches or attacks was low across all three sites. Although staff displayed some awareness of cyberbreaches that have occurred in healthcare more generally, the sites themselves have experienced very few incidents. Those incidents that have occurred were described as minor, e.g., ransomware that had been successfully addressed (without payment) due to backups of the data. No critical incidents had been experienced, with some staff members describing the hospitals as having "been lucky so far". This lack of learned experience may facilitate insecure behaviours. For example, some staff members reflected upon the lack of negative effects they have personally experienced despite using the internet and technology on a daily basis ("well nothing bad has happened so far!"). This could lead staff to underestimate the prevalence of cyberbreaches and/or lead them to feel that their current behaviour must be 'safe' thus reinforcing the behaviour, even if this is not accurate.

Risk Awareness and Lack of Cybersecurity Training

Although many staff were aware that they are expected to behave securely, most demonstrated a lack of understanding why certain behaviours were important. Often, they did not identify potential risks associated with their behaviour. For example, we asked whether staff thought it possible that their own workstation use could affect medical equipment and medical devices in the wider hospital. Generally, staff did not think this was possible nor likely. They did not recognise that they could potentially introduce malware into the wider hospital system. Interestingly, those staff members who *did* identify that it was possible for some workstation use to impact upon medical devices

within the hospital, regarded this as more of an issue for those working in close physical proximity to the medical equipment:

"This is more of a risk for those working near the instruments, e.g., in the surgery"

"[We are] too peripheral to influence things like that. [As we are] so far removed from the medical system"

One staff member explained that they previously acted more securely (e.g., always using their own computer login) when they worked in a department that was more "central to the hospital" as they perceived this to be more vulnerable.

In addition to physical proximity, *type* of computer usage was also perceived to affect risk:

"I only read and see things when I use the computers, I do not input data – therefore I do not see this as a danger [to the system or the hospital]"

This lack of awareness is troubling, and one that should be addressed through staff training and education. A *lack of cybersecurity training* was one of the issues raised by the majority of staff, with many feeling underprepared and unaware of how to use technology securely. Some staff reported receiving no formal computer or cybersecurity teaching and described being self-taught and/or relying on learning by observing their colleagues. In particular, admin staff expressed frustration with their lack of training stating that they felt "out of the loop" and "always the last staff members to be trained (if at all)". One admin staff member described being most likely to be "forgotten about, despite having everyone's' passwords". They felt that they are "not considered important for security" and that this is due to others in their employment not understanding what tasks they actually do (as per our previous discussion on shadow working).

Even some IT staff reported not receiving cybersecurity training and reported using their own initiative to communicate with other colleagues by email to warn about risks they have informally learned about. Therefore, ad-hoc communication – as a result of staff initiative - occurs in some organisations but there is a lack of formal training. Some of the hospital staff did report that new training is being developed and that this is beginning to be rolled out, which will likely include some cybersecurity content.

3.3 Shadow Working Processes

This theme refers to behaviours which are occurring within healthcare institutions to enable efficient working practices, but which are clearly going against policy and in some cases even against country laws such as staff members *sharing login credentials, bypassing official communication channels and remote working.* The staff enact these behaviours in good faith believing they enable their job without a risk to cybersecurity. In some instances, senior management and IT are well aware of these behaviours, but are at a loss as to how these behaviours can be changed.

Sharing Login Credentials

Sharing of personal login credentials was prevalent. Staff regard sharing logins as a necessity in order to complete their daily duties. Unauthorised use of login credentials can actually be classified as a criminal behaviour [23], although it is possible that staff

are not aware of this. A major driver behind the sharing of login credentials is an inconsistency between staff system access levels and the tasks that they are expected to perform by their immediate managers. Administration and junior doctors are restricted in regards to system access privileges, therefore they cannot do a lot of the tasks that senior staff expect of them. However, senior staff do not always have time to do the more administrative elements of their job due to a high workload, time pressure and a focus upon delivering efficient patient care. As one participant states "Surgeons could not do surgery if they spent all their time making appointments". Therefore, to enable them to focus their time more efficiently, senior staff delegate tasks such as prescribing, making appointments, and entering written notes into the system to more junior members of staff. To work around junior staff access restrictions, senior staff members share their own login credentials. In addition to cybersecurity and legal concerns, this behaviour also raises safety concerns. For example, non-medical staff are reportedly entering information from medical notes (including diagnoses) onto hospital systems. Handwritten notes can leave a degree of interpretation, and the staff member inputting the information often has to decide which categories and options they select on the computer system to accurately reflect the patient's condition and treatment. Mistakes could have significant consequences, despite this workaround being driven by staff motivation to improve patient care.

This is a problem that is not easily solved by technology alone, clear governance and workload reduction is required. We must ensure that the true way that hospitals work is recognized, and changes to policy are in place to facilitate effective patient care without putting safety at risk Literature suggests that system design is adding to staff burden through poor usability of all devices and software eg, electronic health records [24].

Bypassing Official Communication Channels

We found evidence of staff bypassing official communication channels and emailing sensitive patient information in an insecure manner. Some medical staff reported e-mailing sensitive patient information (including detailed descriptions of a patient's condition and/or treatment) to a large group of their colleagues. This ensures that all of their colleagues are updated and that all key information about the patient and their current condition is easily accessible and summarised in one place. This raises concerns over the security and privacy of the e-mailed data (e.g., staff indicated that there is a lack of discrimination as to which colleagues are copied into the e-mails, and as aforementioned the data is not encrypted). Furthermore, if information is being sent via e-mail, it is possible that this is not being updated on the central system and therefore vital information may be missed from the patient's electronic health record. Staff also report e-mailing sensitive information to their personal home e-mail to enable them to work from home.

Interestingly, staff at one site described using the smartphone messenger application, WhatsApp, to communicate with their work colleagues. This included using the app to send patient details, test results and/or photos of the patient to one another, in order to ask their opinion. Staff perceive WhatsApp as a quicker, more convenient method to quickly share information/photos, compared to using the official systems. WhatsApp can reduce staff burden, enabling them to focus on patient care (e.g., allowing them to

stay by the patient's bed whilst gathering second opinions rather than leaving to use a workstation). Although this behaviour was only reported at one of the three sites within this sample, previous studies have identified WhatsApp usage at other healthcare sites [25] suggesting this is not an isolated occurrence. Although this method of communication may be quick, convenient and effective – it can also pose security risks when patient data is being sent via a third-party application; particularly one that is often sent and/or received on personal mobile devices and while WhatsApp is encrypted the images may also reside on the phone.

Remote Access and Home Working

Remote access to the hospital network and home working was not the norm, for most staff in our sample. Home working was not an official policy for most sites. However, it is possible for certain members of staff if required – and if authorisation to do so is provided by the IT team. For example, staff responsible for the allocation of organ transplants use remote access to enable them to quickly allocate a donor as soon as an organ becomes available, without first needing to travel to the hospital. For some sites, as a security measure, every remote access connection has to be approved by someone within the hospital (e.g., by calling the hospital and asking another member of staff to press a button to approve the remote access). The IT team at some of the sites are also able to restrict the parts of the system that can be accessed remotely.

In comparison to remote access, saving hospital files onto personal devices to allow home working was reported more frequently. Interestingly some staff commented that even "the chiefs do it" – as social learning theory would predict [Akers, R. L., & Jensen, G. F. (Eds.). (2011). Social learning theory and the explanation of crime (Vol. 1). Transaction Publishers.] the behavior of others is influencing and/or reinforcing this behaviour. Staff report using personal devices on public WiFi networks, for example whilst travelling. Although staff are aware that this could pose some risk, they are also keen to be actively working – and contactable - whilst outside of the hospital; providing another example of a situation where staff feel conflicted between acting securely and productivity.

3.4 Behaviour Prioritisation

Staff demonstrated an awareness that their behaviour differs from that which is expected or advised (shadow behaviours) It is necessary to understand the underlying reasons for this behavior. This theme acknowledges that cybersecurity is often perceived as having low priority compared to other activities required at work. Participants prioritise (i) *productivity and seeing patients*, (ii) *medical expenditure over cybersecurity* and that these priorities are reinforced by (iii) *not enforcing cybersecurity policies.*

Productivity

Cybersecurity measures were often described by staff as counterproductive and time consuming. This is particularly undesirable in a healthcare setting, where patient care is understandably prioritised, and staff are overworked and under severe time pressure

[26]. Anything that is seen as increasing staff burden will be negatively regarded by staff. For example, senior management may restrict staff computer access rights (e.g., to prevent computer settings being changed and new software being installed without an admin login). However, this is often perceived as a barrier to work through preventing installation of required software.

Some staff also felt that security measures may be more focused upon monitoring or restricting staff, rather than improving security for staff and patients. This could potentially affect their motivation to comply. Security measures will also be rejected if quicker workarounds are available, and/or if the measures are not perceived as effective. Due to these negative perceptions of security, particularly as a barrier to productivity and patient-care, senior management and IT technicians described cybersecurity as being a cultural issue – rather than a technical issue; One which requires a "culture change" and a shift in attitudes towards cybersecurity.

Medical Spending Prioritised over Cybersecurity

IT staff acknowledge that the healthcare environment is unique in that priorities must lie with patient care and saving lives – therefore it is not always easy to impose security requirements. They also report a lack of resources and/or budget for cybersecurity. For example, managers were perceived as not allocating adequate budget for cybersecurity, because they want to use this money to purchase something tangible, i.e., "something they can see" such as a hospital bed, or a new medical device. Due to budget constraints, cybersecurity tends to get missed from the business priorities. It was felt that governmental changes may help to prioritise, enforce and regulate cybersecurity.

Lack of Policy and Reinforcement of Safe Behaviour

Staff reported a lack of cybersecurity policies at work, or a lack of reinforcement for any policies that do exist. Staff feel that there is a lack of structural, clear guidance and clarification regarding (un)desirable behaviours. When policies do exist, staff feel that this is unfortunately, never enforced – and conversely good behaviour is never rewarded. Some work places require staff to sign a document to say they will abide by a security policy; however, IT staff feel that new staff often sign this document without actually reading it. IT staff described feeling hopeful that the introduction of the new EU Cybersecurity Act may help to address some of these problems around security policy and reinforcement. The new law imposes that the government identifies 'critical structures' and these structures will have to adopt extra security measures in an allocated period of time. Hospitals are likely to be identified as critical structures. As the law only got approved on the 18th May 2019, IT staff are still in the stage of establishing how to implement the requirements. Therefore, time will tell what impact this will have upon cybersecurity in healthcare.

Staff reported feeling that cybersecurity only becomes a concern if there is a major incident and the employer and/or employees face legal action. For example, one site described how a previous court case found that a patient's surgical report had been rewritten 8 times. This resulted in a new procedure being introduced to monitor and limit amendments to patient data, including the requirement for a clear audit trial. Other

behaviours reported by the staff in our sample could potentially lead to legal action, e.g., sharing of login credentials [23], but this may not be widely enforced.

Interestingly, reinforcement of secure behaviour may also come from unexpected sources. For example, some staff reported acting more securely depending upon the department that they are working in. One employee described only using their own login credentials when they worked in a department that used login times to record employees working hours. Therefore, using logins to record working hours had an unexpected secondary benefit of increasing more secure behaviour through discouraging use of shared login credentials.

3.5 Environmental Appropriateness

This theme explains the ways that the work and systems fail to provide appropriate, flexible, mobile, efficient ways of working that the staff desire, in ways that are deemed secure. There is tension between official secure procedures and what staff see as essential within their work environment and current work culture. One example of this is system readiness. Staff raised concerns about the availability of equipment which led to them being apprehensive about automatic timeout of systems, switching users, and software updates.

No-delay availability

Automatic log-out after a period of inactivity, might improve cybersecurity but it is not implemented across all of the workstations. Auto log-out is not feasible on all computers such as those on the ward, where it could potentially interfere with delivery of patient-care (e.g., if a doctor forgets their login credentials, or logging in and out is perceived to take too much time). For other workstations, even if implemented, auto log-out is ineffectual as the workstation is in constant use (e.g., by different staff).

Current culture and need for change

There was a perception that awareness of cybersecurity issues within the healthcare organisations was low, and needed to be improved. IT staff reported feeling that behaviour is slowly improving due to staff gaining some understanding of cybersecurity issues, but that there is a long way to go before behavior would change. Many staff expressed dissatisfaction at not being kept well informed, nor receiving adequate training. Staff expressed a desire to be "kept in the loop" and in particular to be provided with explanations why – and how - certain behaviours are important for security. They expressed that in order to facilitate behaviour change, it is important that security measures are not just imposed upon staff but that staff are involved in the reasoning behind the changes. Some staff felt that being provided with relatable stories and/or real-life events could help illustrate importance and relevance – particularly as many of the staff have not experienced any adverse effects to suggest that change in their behaviour is necessary. Others felt that new regulations (e.g., GDPR) and policy could help influence behaviour. Staff (include those from IT) also identified that cybersecurity procedures need to be easier to read and more user-friendly, to encourage staff to

read them and to aid comprehension. One staff member suggested that it would be beneficial to have a clear contact within the organisation, such as an easily accessible helpline or cybersecurity champion, who they could approach for more information about cybersecurity issues.

The majority of staff described their place of work as "understaffed and overworked" and for many, being too busy and under major time-constraints was seen as a key driver for unsafe behaviour. Security measures need to be realistic for the healthcare environment, user friendly, and time efficient. Current security measures can often be seen as burdensome, for example multiple login screens can be repetitive, frustrating and time consuming. Staff suggested that it would be beneficial if these systems were more cohesive; for example, if there was an easy way to update passwords (and other information) across all systems without logging into each system individually.

For IT staff, cybersecurity was perceived as a cultural issue. They perceived technical solutions to be available to deal with many cyberthreats, but felt that a culture shift in staff attitudes was needed in order to adequately improve cybersecurity. IT described cybersecurity as an "everyday battle to keep things safe" and often described the elder members of staff – with a lot of experience and numerous years spent working in the healthcare environment – as one of the main groups acting insecurely. Interestingly, they also perceived the youngest and/or newest employees to be acting insecurely, and suggested that there may be different factors influencing each group (e.g., elder staff not liking change or not being familiar with technology and younger staff being inexperienced at work and/or overconfident in their own ability to use technology).

As aforementioned, reinforcement of secure (or insecure) behaviour can sometimes come from unexpected sources. For example, some staff described access to their own personal information as a key motivator to prevent sharing of login credentials. Previously, some hospital systems allowed users to access their personal portal (including salary information) using their main staff login credentials. Staff did not like this as it meant users using their shared login information could see their private details. As a consequence, the system was changed so that personal salary information is now held on a separate system, requiring a separate login. Unknowingly, this change likely removed one of main drivers preventing the sharing of login credentials. This provides food for thought when designing future systems.

In addition to addressing staff behaviour and governmental regulation, staff feel that it would be beneficial for systems to be in place that enable risk assessment of cyberthreat vulnerabilities, in the same manner that organisations can assess other security risks (e.g., physical risks). At the moment they feel that overall cybersecurity is weak as there are no method(s) to assess vulnerabilities. However, all staff described computer systems in healthcare as paramount to their everyday jobs – showing that raising cybersecurity levels is critical.

4 Recommendations for change

This section pulls together recommendations for change to address the issues raised by staff.

Standardisation

- Password security options have evolved from the traditional view of secure passwords, to three random words which can be easier to remember (https://www.cyberessentialsonline.co.uk/the-latest-password-guidance-from-the-ncsc/). The medical community should agree a format (similar to how the finance industry consolidated on PIN format) and ensure all medical equipment universally follow that guideline.

Research

Research is needed in the following areas:

- Securing legacy devices is a non-optional priority. Guidance on security, pre and post market, for medical devices is relatively new (e.g. MDCG 2019-16 in Europe) and must be fully implemented into the development and post-market monitoring environment.
- To identify a different policy for managing passwords. Changing passwords should not just be based on time elapsed (i.e., requiring periodic change). The hospital must also ensure they passwords are properly encrypted and that staff have a separate and strong password for email, which if hacked can be used to launch a phishing attack.
- As technology improves and less phishing emails are getting through to staff, paradoxically it is harder for people to detect a phishing email in a low signal environment [27]. If 100% elimination cannot be guaranteed, more research is required to establish an optimal level of fake phishing emails. This level can be maintained through phishing simulation training, to optimise human detection.
- More work is need to establish how to effectively manage updates in relation to two key issues. Firstly, how to effectively schedule updates in 24/7 environments. Secondly, how to accurately predict downtime and ensure it is easy to recover if an update disrupts a system.
- Research is required to explore how best to provide feedback to staff regarding the constant threat their establishment is under and the effectiveness of their behaviour, without creating an environment of constant fear that leads to dysfunctional coping and stress. This should be mindful of findings relating to Protection Motivation Theory [28] and the need to emphasise coping behaviours alongside threat information [29].

Technology improvements

- Allow the local administrator to manage 'remember me' function and similar functions which impact security. This will enable the removal of options such as remember me if this does not comply with local policies.
- Explore means of enabling automatic change of user when staff physically move away from a device. More ethnographic research is required to establish how to maintain context (e.g., current patient record), when login changes between staff working on the same patient case.
- An alternative, mobile, secure channel must be provided to support data transfer between people and locations. This is required for activities such as working from home, bringing in research and presentations to supervisors, and patients bringing in medical records.
  - A secure app, running on a smartphone which is approved by the medical industry and links directly to the electronic health records is needed to ensure central information is up-to-date, easy to share between staff, and does not disrupt working at the patient bedside.
- Encryption tools must be readily available and easy to use. Staff should be trained how to use these tools and made aware of the importance of encryption.
- HCI must ensure that the design of all software is optimised to reduce the burden on staff. Usability, and consistency across device interfaces is key to reduce burden on staff, as well as for any security components.

Ultimately, all tools must be easy to use and not add to the psychosocial stress of the healthcare staff.

5 Conclusion

Our overall findings suggest that insecure behaviours are commonplace across healthcare organisations, on an international scale; and awareness of the breadth of risks associated with these behaviours is generally low. Staff are aware of the external threats but not necessarily how their behaviours facilitate these threats. Awareness training is required to ensure that staff are more aware of the potential implications of their behaviour in the workplace. Staff within healthcare work within a very fast-paced and potentially stressful environment, with a lot of time pressures and responsibilities that do not always facilitate secure behaviour. Current behaviours are engrained habits which coexist with a practical rationalisation that they are required to facilitate efficient patient care. Without awareness of what constitutes unsafe/risky behaviour and the potential consequences (including a lack of learned experience), it is not realistic to expect staff to behave securely. It is vital that they are clearly informed by their employer of what is expected of them, and *why*; and who to approach if they require any further information or guidance.

The administrators and junior medics in our interviews reported feeling as if their roles were not recognised or were regarded as unimportant. In addition to being demoralising for staff, this can also result in staff members not receiving adequate training.

This is driven by shadow working, i.e., a discrepancy between the responsibilities covered in their official written job description, and the tasks that they *actually* conduct on a daily basis. These shadow work processes create a security weakness, in addition to potentially having a negative impact on staff wellbeing through a lack of recognition. We see this as a key area for improvement that requires further understanding of the organisational culture which has led to the existence of these shadow behaviours. Such recognition could be made in different ways, from the introduction of the role of medical scribes to acknowledged responsibility for junior medics and remove the burden from senior medics.

Due to the unique working environment within healthcare, there are limitations on the type of technological interventions which can be introduced. For example, it is not feasible to impose auto log-off on workstations where emergency access is required, nor to require staff to take several steps to access one system. It is vital that any interventions are user-friendly, time-efficient and non-burdensome; otherwise they will – at best, be ineffective (e.g., promoting staff to find 'workarounds') – or at worst, negatively impact upon patient care and/or wellbeing. This need for quick, convenient systems is seen in the workarounds that staff have created, e.g., use of WhatsApp.

Some issues may be more straightforward to, at least partially, address from a technological perspective, such as the use of USB devices and sharing of attachments. For example, screening USB devices on machines that are isolated from the main hospital network. However, it is still important that staff are kept informed of the importance and rationale behind these interventions. This will help to help facilitate their adoption and continued use, and minimise perceptions of security as simply a barrier to productivity and another "hoop to jump through" for no perceived reason or reward.

In conclusion, the findings from this study highlight a range of insecure behaviours currently occurring within healthcare environments. No technology is a silver bullet ready to reduce cybersecurity risks. Rather, this complex socio-technical will be solved by understanding the underlying reasons for behavior, implementation of appropriate processes and appropriate design of technology.

These findings have implications for the design of both behaviour change interventions aiming to promote secure behavior and the design of technology itself to ensure that the secure use of technology is as easy as the insecure and not adding to the psychosocial stress of the users. Further research should focus upon potential intervention techniques, including gathering feedback from healthcare staff around perceived appropriateness, feasibility and acceptance. Engagement of the clinical leadership to shift cybersecurity conversations from technical to one linked to patient safety and organizational resilience is needed. This means presenting cybersecurity data in terms of clinical and business outcomes.

References

1. Kotz D, Gunter CA, Kumar S, Weiner JP (2016) Privacy and Security in Mobile Health: A Research Agenda. Computer (Long Beach Calif) 49:22–30. https://doi.org/10.1109/MC.2016.185

2. Burns AJ, Johnson ME, Honeyman P (2016) A brief chronology of medical device security. Commun ACM 59:66–72. https://doi.org/10.1145/2890488
3. Coulter A, Roberts S, Dixon A (2013) Delivering better services for people with long-term conditions. Building the house of care.
4. Hedström K, Karlsson F, Kolkowska E (2013) Social action theory for understanding information security non-compliance in hospitals the importance of user rationale. Inf Manag Comput Secur. https://doi.org/10.1108/IMCS-08-2012-0043
5. Shenoy A, Appel JM (2017) Safeguarding confidentiality in electronic health records. Cambridge Q Healthc Ethics 26:337–341. https://doi.org/10.1017/S0963180116000931
6. Coventry L, Branley D (2018) Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas 113:48–52. https://doi.org/10.1016/j.maturitas.2018.04.008
7. (2019) Systems shut down in Victorian hospitals after suspected cyber attack. Guard.
8. Albert M (2019) "Why do we need to wait for people to be hurt?" Medical cyber attacks soar 1400%. In: SFGate. https://www.sfgate.com/healthredesign/article/medical-cyber-attacks-terrorism-hospital-health-13853912.php. Accessed 11 Oct 2019
9. Kam R (2015) The human risk factor of a healthcare data breach - Community Blog. In: Heal. IT Exch. https://searchhealthit.techtarget.com/healthitexchange/CommunityBlog/the-human-risk-factor-of-a-healthcare-data-breach/. Accessed 10 Apr 2018
10. Scott M, Wingfield N (2017) Hacking attack has security experts scrambling to contain fallout. New York Times
11. National Audit Office (2018) Investigation: WannaCry cyber attack and the NHS
12. Sussman B (2019) Doctors Quitting Due to Ransomware Attacks. In: SecureWorld. https://www.secureworldexpo.com/industry-news/are-doctors-quitting-after-ransomware-attacks. Accessed 30 Jan 2020
13. Zimmermann V, Renaud K (2019) Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. Int J Hum Comput Stud 131:169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005
14. Boyce MW, Duma KM, Hettinger LJ, et al (2011) Human performance in cybersecurity: A research agenda. In: Proceesings of the Human Factors and Ergonomics Society 55th Annual Meeting. pp 1115–1119
15. Hall LH, Johnson J, Watt I, et al (2016) Healthcare Staff Wellbeing, Burnout, and Patient Safety: A Systematic Review. PLoS One 11:e0159015. https://doi.org/10.1371/journal.pone.0159015
16. Hall LH, Johnson J, Heyhoe J, et al (2017) Exploring the Impact of Primary Care Physician Burnout and Well-Being on Patient Care. J Patient Saf 1. https://doi.org/10.1097/PTS.0000000000000438
17. Johnson J, Hall LH, Berzins K, et al (2018) Mental healthcare staff well-being and burnout: A narrative review of trends, causes, implications, and recommendations for future interventions. Int J Ment Health Nurs 27:20–32. https://doi.org/10.1111/inm.12416
18. Bridgeman PJ, Bridgeman MB, Barone J (2018) Burnout syndrome among healthcare professionals. Am J Heal Pharm 75:147–152. https://doi.org/10.2146/ajhp170460
19. Zaccaro SJ, Dalal RS, Tetrick LE, et al (2016) The Psychosocial Dynamics of Cyber Security: An Overview. In: Psychosocial Dynamics of Cyber Security. Routledge, pp 31–42
20. Blythe JM (2013) Cyber security in the workplace: Understanding and promoting behaviour change. In: Proceedings of CHI 2013 Doctoral Consortium
21. Vossler A, Moller N, Braun V, et al (2017) How to use thematic analysis with interview data. In: The Counselling and Psychotherapy Research Handbook

22. Williams B (2019) The dangers of password sharing at work. In: TechRadar. https://www.techradar.com/news/the-dangers-of-password-sharing-at-work. Accessed 14 Oct 2019
23. Caldwell F (2016) Why Sharing Passwords Is Now Illegal And What This Means for Employers And Digital Businesses
24. Zahabi M, Kaber DB, Swangnetr M (2015) Usability and Safety in Electronic Medical Records Interface Design: A Review of Recent Literature and Guideline Formulation. Hum Factors 57:805–834. https://doi.org/10.1177/0018720815576827
25. Johnston MJ, King D, Arora S, et al (2015) Smartphones let surgeons know WhatsApp: An analysis of communication in emergency surgical teams. Am J Surg. https://doi.org/10.1016/j.amjsurg.2014.08.030
26. Coventry L, Branley-Bell D, Magalini S, et al (2020) Cyber-risk in healthcare: Exploring facilitators and barriers to secure behaviour. In: Lecture Notes in Computer Science
27. Sawyer BD, Hancock PA (2018) Hacking the Human: The Prevalence Paradox in Cybersecurity. Hum Factors 60:597–609. https://doi.org/10.1177/0018720818780472
28. Briggs P, Jeske D, Coventry L (2017) Behavior Change Interventions for Cybersecurity. In: Behavior Change Research and Theory: Psychological and Technological Perspectives. Academic Press, pp 115–136
29. Witte K, Allen M (2000) A meta-analysis of fear appeals: Implications for effective public health campaigns. Heal Educ Behav 27:591–615. https://doi.org/10.1177/109019810002700506