Chartered Institute
of Ergonomics
& Human Factors

Human Affected Cyber Security (HACS) Framework

WHITE PAPER

#ciehf

Executive Summary

Cyber security incidents cause damage to organisational reputation, finances, and national security. Many incidents have been attributed to the human element or "insider threat". Therefore, addressing cyber security, without considering the human element, would be like locking all the windows on your house but leaving the front door wide open. Mature organisations recognise that systemic failures are usually the cause of incidents. It is also important to recognise that the human element can strengthen cyber security.

Financial costs of cybercrime have been estimated as $945 billion worldwide (approximately £680 billion)[1]. In the UK, the maximum fine for a General Data Protection Regulation (GDPR) breach is £17.5 million or 4% of annual turnover (whichever is greater). As well as direct financial losses, indirect financial loss can be caused by damage to reputation and customer confidence, or cyber espionage and the associated loss of commercially-competitive product design information to a competitor. National security is under threat from state actors using cyber security attacks.

A practical framework presents specified, undesirable behaviours and associated solutions. The framework can be used proactively, to assess and mitigate cyber security risks, and retrospectively, to identify potential human-related incident causes. It includes "risky behaviours" in the following categories:

1. **User validation violations**
2. **Information sharing**
3. **Misuse of technology**
4. **Training**
5. **Poor monitoring and incident management**
6. **Neglecting physical environment security**
7. **Deliberate, malicious attack.**

Behaviour-related causes in the framework pertain to organisational culture, ways of working, situational factors and the influence of the physical environment. A smaller group of individual causes; factors associated with individual people, are also presented. However, the recommended solutions largely pertain to changes at a system or organisational level. By addressing these systemic, organisational failures, the risk of human-related cyber security incidents can be reduced.

[1] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

Contents

1.0 Introduction

1.1 Aims of paper

Cyber security incidents have caused damage to organisational reputation, finances, and national security. Many incidents have been attributed to the human element or what is referred to now as "insider threat". However, mature organisations recognise that systemic failures are usually the cause of incidents. It is also important to recognise that certain human skills can strengthen cyber security. This paper presents a practical human factors (HF) framework that can be applied to enhance cyber security (Table 1). The Human Affected Cyber Security (HACS) framework incorporates risky behaviours, causes and solutions.

1.2 Who should read this paper?

This paper is designed to support HF practitioners, particularly those with an interest in human reliability analysis (HRA) who may wish to apply similar methods to a cyber security context. It may also interest cyber security professionals who would like to know more about the contribution of the human element.

A separate CIEHF paper will provide further HF guidance to support policy makers, chief information security officers (CISOs) and other cyber security professionals.

2.0 Problem definition: why do we need to consider HF in cyber security?

2.1 Cost of cyber security incidents

The Centre for Strategic and International Studies, in partnership with the computer security company McAfee, presented a paper that projected the cost of cybercrime as $945 billion in losses worldwide[2]. In the UK, financial consequences of an information breach can be indicated by General Data Protection Regulations (GDPR). The maximum fine for a GDPR breach is £17.5 million or 4% of annual turnover (whichever is greater)[3]. As well as direct financial losses, indirect financial loss can be caused by damage to reputation and customer confidence, or cyber espionage and the associated loss of commercially competitive product design information to a competitor.

In addition to the financial losses of commercial organisations, national security is also under threat from state actors using cyber security attacks. Depending on the scale and intensity of the attack the effect can be devastating for countries, organisations and individuals alike.

2.2 Human factors - related causes of cyber security incidents

Regardless of the scale of a cyber security incident, there is growing acknowledgement that the contribution of HF, and management of the associated human strengths and vulnerabilities, is key to robust cyber security protection and prevention. A large proportion of cyber security incidents are attributed to human error or insider threat. For example, Cybint Solutions (2020) found "95% of cyber security breaches are due to human error". IBM[4] reported that "Insider incidents made up 13% of all OT (Operational Technology) -related incidents in 2020, with about 60% of those involving malicious insiders and about 40% involving negligence". The previous year's report found "over 8.5b records were compromised in 2019 … The inadvertent insider can largely be held responsible." In 2019, a CybSafe analysis of cyber data indicated that 90% of cyber breaches were due to human error[5]. However, the terms "insider threat" and "human error" may distract from the systemic, organisational failures that are at the root of such incidents.

2.2.1 What is insider threat?

The term insider threat could give the impression that employees are to blame for cyber security incidents, so it may be useful to explore what it really means. Building on Pollini et al (2021)[6], three types of insider threat are described in the follow paragraphs:

- Unintentional, non-malicious
- Intentional, non-malicious
- Intentional malicious.

HF professionals who work to enhance safety will be familiar with the principles of the former two types. However, the third type; intentional malicious behaviour, is a relatively new area. Solutions to address insider threat, in terms of risky behaviours and systemic causes, are presented in the HACS Framework, in Section 3.0.

[2] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf
[3] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/penalties
[4] IBM X-Force Threat Intelligence Index 2021
[5] https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
[6] Pollini A., Callari, T., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., Guerri, D., (2021). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology and Work.*

2.2.1.1 Unintentional, non-malicious insider threat

Rasmussen's (1983)[7] classic taxonomy of human error describes skill-based, rule-based and knowledge-based behaviours.

In cyber security, skill-based errors may contribute to email vulnerability. A memory lapse or lack of conscious thought can cause people to inadvertently activate malicious email links and applications. Time pressure and poor email management can exacerbate this. Similarly, contextual bias may explain the success of whaling and spear-phishing emails, which are designed to target individuals on the basis of their known interests or work context. The recent municipality attack on Brescia, Italy is an example of this type of attack. (See box 1). Slips and lapses can account for loss of sensitive information in laptops or paperwork. Forgetting to update software is another example of an unintentional error.

BOX 1 Brescia municipality attack, 2021[8]

What happened?
A 'DoppelPaymer' ransomware attack was conducted on the Municipality of Brescia, Italy, causing data to be encrypted and denial of services.

Consequences
As a result, the municipality website including tender and contracts, schools and cemetery systems, was blocked for several days. Accountancy, registry and local police computer workstations were also blocked. Eventually, back-ups were restored. Days after the attack, stolen data from the municipality appeared on darknet websites, with the attackers threatening to disclose other stolen data if a ransom of approximately 1.3 million Euros was not paid.

Causes
The ransomware was contained in malicious emails. Users opened links or attachments and inadvertently activated the ransomware.

HF lessons
In this example, the human element appears to be the weak point, however, wider organisational factors need to be considered. It is essential to train employees how to recognise phishing attempts. They should be provided with a simple, efficient means of reporting suspicious emails. An investigation of email management and job design may also reduce the risk of recurrence.

[7] Rasmussen, J. (1983). Skills, Rules, and Knowledge: Signals, Signs, and Symbols, and other Distinctions in Human Performance Models. *IEEE Transactions on Systems, Man, and Cybernetics, SMC-13(3), 257-266.*
[8] https://www.privacy365.eu/en/hackers-ask-for-a-ransom-of-13-million-euros-the-informatic-system-of-the-brescia-municipality-is-paralyzed-by-a-ransomware/

The social 'rule', that it is polite to hold doors open, may be inappropriate in a secure environment that is restricted to authorised personnel. Malicious outsiders can gain unauthorised access to a secure building in this way. Similar sociable behaviours, such as sharing information on social media and in other non-work environments, can result in unintentional breaches of sensitive information. Social compliance also creates greater vulnerability to coercion by a malicious colleague or external personnel. It could be a factor in the banking attack described in box 2.

Some personality types may be more susceptible to cyber attacks. For example, someone with a high degree of social compliance or agreeableness may be more likely to share information or hold doors open for others. In many settings this contributes to a pleasant and productive working environment, however, under the wrong circumstances it may also introduce security risks. Taking the opposite perspective, someone with a high sense of duty may be more likely to follow cyber security/information management procedures (Gratian et al. 2018[9]; Hadlington 2018[10]; Jeong et al. 2019[11], Widdowson, 2019[12]). Personality is considered to be generally stable throughout life (Mõttus et all 2012[13]), although testing should be repeated every two years by a qualified psychometric tester.

A lack of knowledge of cyber security procedures, or even awareness of the existence of cyber security procedures, can result in related errors. This, in turn, could be caused by organisational failures such as inadequate provision of cyber security training, procedures that are not designed around work as it is performed, or procedures that are difficult to access.

[9] Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. computers & security, 73, 345-358.
[10] Hadlington, L. J. (2018). Employees attitudes towards cyber security and risky online behaviours: an empirical assessment in the United Kingdom.
[11] Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019). Towards an improved understanding of human factors in cybersecurity. In 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC) (pp. 338-345). IEEE.
[12] Widdowson, A.J. (2019). 9 factors for reducing insider threat and enhancing cyber security (Thales whitepaper, and in *The Ergonomist* Sept-Oct 2019 edition)
[13] Mõttus, R., Johnson, W., & Deary, I. J. (2012). Personality traits in old age: Measurement and rank-order stability and some mean-level change. Psychology and Aging, 27(1), 243–249, https://doi.org/10.1037/a0023690, https://doi.apa.org/doiLanding?doi=10.1037%2Fa0023690

BOX 2 Barclays-Santander banking attack, 2013

What happened?

Cyber criminals entered branches of high street banks and pretended to be from the company's IT department. Bank staff gave them access to their computer system. They installed a KVM (keyboard, video, mouse) switch which allowed them remote access to the bank's computer[14].

Consequences

The attackers were able to access customer personal data such as credit and debit card details, putting them at risk of further crime, and withdrew £1.25 billion. The gang were caught by police and most of the money was recovered. The news coverage likely resulted in reputational damage for the bank and raised questions about security.

Causes

It is important to note that the incident wasn't restricted to one banking organisation or one branch. This suggests that human error and associated organisational root causes may have been responsible. Diffusion of responsibility, where each individual staff-member's failure to check the attacker's credentials confirmed the lack of action by the others[15]. The tendency to trust people that we like[16] and social compliance may have also contributed to the failure to check credentials.

HF Lessons

Instead of blaming the staff-members who directly interacted with the attackers, training and improved visitor management policy could reduce the risk of a recurrence of this type of incident. Training recommendations are presented in the HACS framework.

This attack was one of the original incidents that formed the foundation assessment of the Cyber Human Error Assessment Tool (CHEAT®)[17]. It illustrates that even a system with strong technical controls can be overridden by human operators.

[14] https://news.sky.com/story/barclays-cyber-raid-arrests-over-stolen-1-3m-10433789 https://www.bbc.co.uk/news/uk-england-london-27146037

[15] Rosenbaum M.E, Blake R.R. (1955). Volunteering as a function of field structure *Journal of Abnormal and Social Psychology,* 50, pp 193-6.

[16] Eagly, A.H, Chaiken, S. (1984). Cognitive theories of persuasion in L. Berkowitz (ed.) *Advances in Experimental Social Psychology*, 17, Orlando, Fla.: Academic Press (pubs).

[17] Widdowson, A.J., Goodliff, P.B. (2015). CHEAT, an approach to incorporating human factors in cyber security assessments, IET System Safety and Cyber Security conference, UK

2.2.1.2 Intentional, non-malicious insider threat

Behaviours in this category are deliberate "violations" of cyber security policy or procedures. However, they are performed in an attempt to get the job done in a more efficient manner. If cyber security policy and procedures are too strict, employees may find workarounds. Beautement et al (2008) describe a "compliance budget"[18]; a cost-benefit analysis that results in people either choosing not to comply with security measures, or finding more efficient workarounds. For example, if employees are prevented from sharing necessary information with third parties, they may resort to the use of personal email or removable memory devices that are not protected by internal Information Security (IS) controls. Procedures need to be designed around work demands.

Another violation is using the same easy-to-guess password for multiple personal and professional applications, or storing the password unsafely. The systemic cause is the need to remember many passwords, which places unreasonable demands on human memory capacity. Alternative user authentication solutions, such as biometrics, are advisable. Poor password practices were identified as the cause of the Great Western Railway (GWR) incident in 2018 (See box 3).

BOX 3 Great Western Railway, 2018

What happened?
In April 2018, Great Western Railway (GWR) discovered that around 1,000 of its passengers' login details had been compromised by hackers. The security staff determined that the hackers subsequently used the passengers' passwords elsewhere.

Consequences
While GWR were able to shut this activity down quickly and contact those affected, a small proportion of accounts were successfully accessed. As no usable bank data was stored on the GWR website, the train operator confirmed that the leakage of bank details couldn't have occurred. A UK news resource confirmed that the leaked passwords were now available on the dark web where interested hackers made a bid to acquire those passwords to later use them for malevolent purposes. Hence, GWR advised the customers to change their passwords as soon as possible. The company also took steps to isolate its database from future cyber threats[19]. The incident revealed ticketing to be a highly exposed rail information system with similar vulnerabilities to those faced by websites (e.g. with payment services).

Causes
The incident was attributed to poor password practices.

HF Lessons
Current systems rely on people to use a different, complex password for each online service they use. However, this is reliant on human memory capacity. Alternative user authentication methods such as biometrics, are recommended where possible.

[18] Beautement, A., Sasse, M. A., & Wonham, M. (2008). The compliance budget: managing security behaviour in organisations. In Proceedings of the 2008 New Security Paradigms Workshop (pp. 47-58).

[19] https://www.cybersecurity-insiders.com/cyber-attack-on-great-western-railways/ https://www.bbc.co.uk/news/technology-43725640

Employees often engage in a range of behaviours including non-compliance and shadow security, (employee workarounds that are not "compliant" but may afford some level of security)[20], culminating in risky security behaviours. Motivational factors, like self-efficacy, are consistently found to be important for driving security behaviours across contexts[21]. However, efforts to enhance people's risk perceptions (e.g., perceived severity and perceived susceptibility of security threats) only have small, and inconsistent, effects[22]. Other research supports the role of organisational factors like employee trust[23], perceptions of responsibility[24], and social influences[25] to be important for facilitating cyber security behaviours. HF solutions to address these behaviours are described in the HF Cyber Security Framework.

2.2.1.3 Intentional, malicious insider threat

Deliberate, malicious cyber security attacks are motivated by a variety of goals. Employees within an organisation who attempt to share sensitive information or disrupt/damage internal systems, may do so for a number of reasons. They may feel overlooked and unappreciated; they may have financial difficulties or be facing redundancy; or they may disagree with management decisions. Malicious insider behaviours have been categorised as negligence (Hadlington, 2018[26]) and sabotage (Thaduri et.al., 2019[27]); and are often conducted by rogue employees (Ghafir et al. 2018[28]). According to routine activity theory, crime requires three main conditions: a motivated offender, a suitable target (e.g. a project or the organisation as a while) and the absence of a capable guardian[29]. Clough[30] defines guardianship roles in terms of humans watching, enforcing, and supporting. It is important to remember that people can change since any initial screening during recruitment. Susceptible employees such as these may be targeted by malicious insiders or outsiders and persuaded to take part in a cyber security attack. Methods of persuasion may include blackmail, bribery or making the target feel important and appreciated. External attacks are initiated by individuals or highly organised crime organisations (Abbott et al., 2015). Motivations include political beliefs, state attacks, finance, commercial espionage, or simply fun. An example attack, that appeared to be financially motivated, targeted coronarvirus vaccine work at Oxford University (See box 4).

[20] Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security.

[21] ENISA (2018). Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity.

[22] Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. International. Journal of Information Security and Privacy (IJISP), 9(1), 26-46.

[23] Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. Computers & security, 31(4), 597-611;

[24] Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. In Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015) (pp. 103-122).

[25] Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. International. Journal of Information Security and Privacy (IJISP), 9(1), 26-46.

[26] Hadlington, L. J. (2018). Employees attitudes towards cyber security and risky online behaviours: an empirical assessment in the United Kingdom.

[27] Thaduri, A., Aljumaili, M., Kour, R., & Karim, R. (2019). Cybersecurity for Maintenance in railway infrastructure: risks and consequences. International Journal of System Assurance Engineering and Management, 10(2), 149-159.

[28] Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., ... & Baker, T. (2018). Security threats to critical infrastructure: the human factor. The Journal of Supercomputing, 74(10), 4986-5002.

[29] Cohen, LE, Felson, M, 1979, "Social change and crime rate trends: A routing activity approach", American Sociological Review 44 (4): 588-608

[30] Clough, J. (2015). Principles of cybercrime. Cambridge University Press.

BOX 4 Coronavirus vaccine attack, 2021[31]

What happened?

An Oxford University laboratory was attacked. Machines used to purify and prepare biochemical samples like those used in coronavirus research, were hacked.

Consequences

Attackers gained the ability to control the pumps and pressure and sabotage research.

Causes

In May 2020, the UK National Cyber Security Centre (NCSC) reported large scale ‘password spraying’ campaigns against healthcare bodies and medical research associations. Password spraying uses the same password to attempt to access multiple accounts. This may have been a cause of the incident. The attack may have been financially motivated, as vaccine information was very valuable at the time.

HF Lessons

This attack further illustrates password vulnerability. People may use common, easy-to-guess passwords because they have difficulty remembering multiple login-details for all their personal and professional applications. Alternative user authentication methods, such as biometrics, could alleviate this.

[31] https://www.standard.co.uk/news/uk/hackers-oxford-university-coronavirus-research-lab-cyber-attack-b921297.html

3.0 Human Affected Cyber Security (HACS) Framework

HACS is a practical framework, or checklist, designed to capture specified, undesirable behaviours and associated solutions.

3.1 The need

As described earlier, in section 2.0, cyber security incidents can be costly in terms of reputation, finance and even national security. The human-element in an organisation, also known as 'insider threat', can be harder to predict and change than the technological elements. A successful attack is the result of several factors related to both individual and organisational elements like policies, culture, and practices of an organisations[32]. In order to address human vulnerabilities, it is necessary to address systemic failures. This framework addresses individual and organisational factors that contribute to cyber security violations.

3.2 Purpose

The primary purpose of this framework is to provide a structure to capture people-related cyber security vulnerabilities in organisations, causes and mitigating solutions. It can be used proactively, as part of a cyber security risk assessment, or retrospectively, in an incident investigation. The framework should be seen as a starting point for HF practitioners to adapt as technology and working practices evolve, and as new research is published.

3.3 Framework development background

Initial vulnerabilities were identified from the Cyber Human Error Assessment Tool (CHEAT®)[33]. They were developed based on the application of social, cognitive and organisational psychology and safety incident investigation principles to open-source cyber security incidents, to identify HF root causes. One of the incidents affected two banking organisations, Barclays and Santander, and was described earlier (see box 2). These vulnerabilities were extrapolated into risky behaviours; human actions or inactions that increase susceptibility to cyber-attacks. They were further developed and documented in a table format.

3.4 Framework structure

The framework presents risky behaviours, organisational causes, individual causes, quick wins, and long-term solutions. The behaviours described are applicable to any size of organisation, including Small and Medium-sized Enterprises (SMEs). They are focussed on human actions or inactions, rather than technical vulnerabilities. However, some of the causes and solutions are heavily related to human interaction with technology.

[32] Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. Computers & Security, 23(3), 253-264.

[33] Widdowson, A.J., Goodliff, P.B. (2015). CHEAT, an approach to incorporating human factors in cyber security assessments, IET System Safety and Cyber Security conference, UK
Widdowson, A.J. (2016). CHEAT® and updated approach to incorporating human factors in cyber security assessments, Engineering and Technology Reference, 6 pp. Online ISSN 056-4007
Widdowson, A.J. (2017). Human factors in rail cyber security, Sixth international rail human factors conference, London, UK (available on RSSB's SPARK website)
Widdowson, A.J. (2019). 9 factors for reducing insider threat and enhancing cyber security (Thales whitepaper, and in The Ergonomist Sept-Oct 2019 edition)

3.4.1 Risky behaviours

RISKY BEHAVIOURS WERE GROUPED INTO SEVEN CATEGORIES:

1. **User validation violations** (password management)
2. **Information sharing** (in person and online)
3. **Misuse of technology** (e.g., use of compromised devices and websites)
4. **Training** (failure to undertake training)
5. **Poor monitoring and incident management** (asset management and failures in reporting, investigating and learning from incidents)
6. **Neglecting physical environment security** (e.g., allowing tailgating, leaving sensitive documents in view, securing access to servers and networks)
7. **Deliberate, malicious attack.**

More details about the categories and associated solutions are presented in the following paragraphs.

1. User validation violations

The use of passwords for user validation is heavily reliant on limited human memory capacity. A typical user will require many passwords for personal and professional applications and websites. There is a risk that people will use the same, easy to remember password for several applications, creating a single point of failure, share them with others, or store the passwords unsafely. Provision of password safes can help. However, better solution may involve the use of technical alternatives technologies such as biometrics.

2. Information sharing

This category encompasses ways information sharing creates vulnerability. Information shared in public areas and online gives attackers insights into an organisation, its products and capability. Sharing on social media platforms provide cyber criminals with the means to target individuals with malicious emails, a practice known as spear-phishing or whaling. These vulnerabilities can be addressed by monitoring and open-source intelligence surveys. If cyber security policies and procedures are too strict, employees are likely to find workarounds, such as sending information using their personal email accounts, or unauthorised use of peripheral devices such as USB memory drives. The procedures need to be designed around jobs and, if possible, the most secure way to perform a task should also be the easiest way.

3. Misuse of technology

Use of unauthorised, equipment, internet sites and public WI-FI are included in this category. Asset management, including software updates and patching, and restrictions on unapproved software downloads, are also considered.

4. Training

This category includes failure to complete cyber security training. Reasons include a lack of accessible, well-designed, relevant training. A competence management system can be used to monitor training completion and understanding.

5. Poor monitoring and incident management

Learning from cyber security incidents in dependent on reporting. Employees need to be able to report incidents easily and without fear of blame or punishment. Significant or common incidents should be monitored, investigated and associated lessons, captured and applied. Incident investigation should cover HF considerations such as those in the framework, with the help of a competent HF practitioner. Organisations need to be prepared to respond to an attack.

6. Neglecting physical environment security

Although it may not seem like an obvious part of cyber security, an important attack route, especially for 'air-gapped' systems which are not connected to the Internet, is the physical working environment. Attackers may gain unauthorised access by 'tailgating'; following authorised personnel through entry points. They then seek access to electronic systems by unlocked computers, inserting USB devices and access information from paperwork left on desks, printers or in unlocked storage facilities. The security of remote working environments also needs to be considered. An understanding of HF can help identify and reduce the vulnerability of the physical environment. If people are used to seeing strangers in their working environment, they might be less likely to challenge an unauthorised attacker. Good visitor identification and management can mitigate this. Tailgating can be mitigated by turnstiles and/or security personnel at entry points. Politeness can prevent individuals from checking credentials before allowing access so clear allocation of this responsibility to security personnel is advisable.

7. Deliberate, malicious attack

Although the majority of insider threat incidents are caused by non-malicious behaviours, the framework also addresses the causes of deliberate attacks and how the risk can be mitigated. If employees feel unappreciated, at risk of redundancy or disagree with an organisational policy, for example, the risk of them compromising the organisation increases. It is, therefore, prudent to provide emotional support mechanisms, assess morale using engagement surveys and conduct monitoring.

FOR FURTHER DETAILS ABOUT THE CATEGORIES, SEE TABLE 1.

3.4.2 Behavioural causes

Likely root causes of these risky behaviours are described in the ‘Organisational causes’ and ‘Individual causes’ columns in the tables. Without HF consideration in incident investigation, the root cause can be misleadingly labelled as human error. This only addresses individual factors, (such as memory failure, personality and lack of ability), and unfortunately does not provide much insight into how to reduce the likelihood of the incident happening again. It is therefore necessary to identify systemic, organisational causes, and solutions. Organisational causes are addressed in terms of ways of working (policies, processes, design of technology and jobs); culture (shared beliefs and values within the organisation); physical environment (office or building layout that can influence risk), and situational factors (external elements that influence risky behaviours).

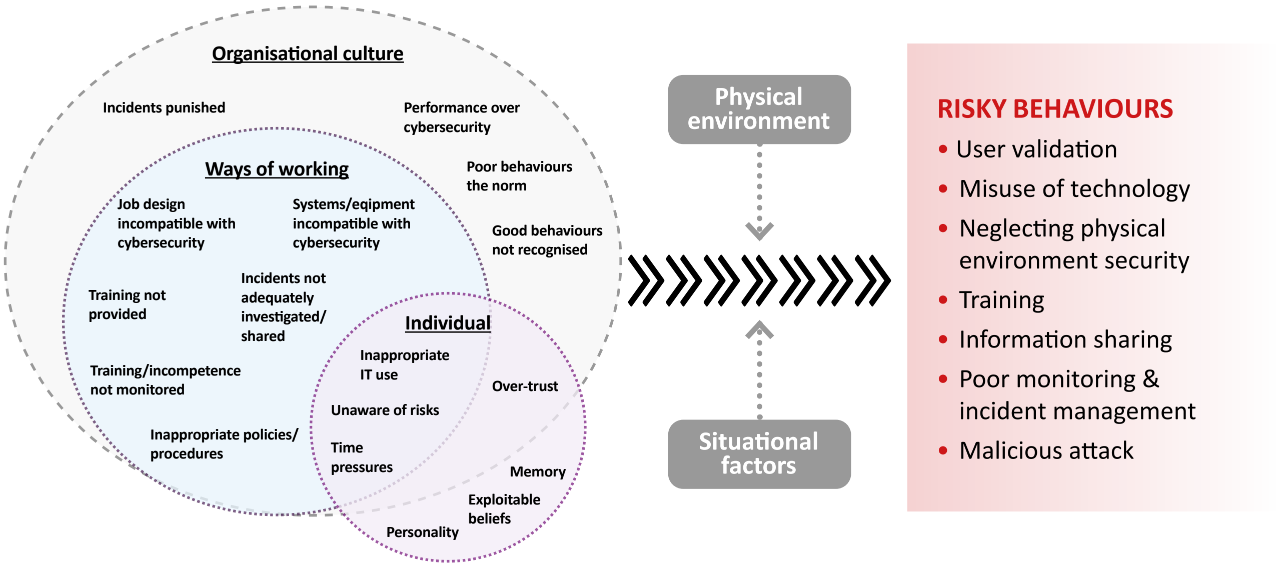
3.4.2.1 Interaction between causes

The framework captures detail on risky behaviours, their organisational and individual causes, and potential solutions as described in the previous section (3.4). When reading information in a table format it may be easy to assume that items are independent and can be treated in isolation to each other. Figure 1 illustrates that there are many interactions between the causes of, and, therefore, solutions to, risky behaviours.

The diagram shows the direct causes of risky behaviours as a combination of organisational culture, ways of working, and individual factors. There are some individual causes outside organisational culture or ways of working, such as memory capacity and personality, but individual behaviours can also be affected by the organisational factors, as illustrated. Over-trust is an example of this. Experience has shown that employees can assume their IT department will protect them from cyber security threats. In a mature culture, all personnel take responsibility for cyber security. Culture can be enhanced by management endorsement and role modelling. Rewards and recognition mechanisms need to address good cyber security behaviours; not just productivity.

There are overlaps between categories. For example, a failure to complete training about cyber security risks could cause other risky behaviours such as inappropriate use of technology. It is important to understand that there are multiple causes of certain behaviours. The table indicates potential causes, although to fully understand why a behaviour occurs, an analysis of the specific drivers behind that behaviour should be conducted.

Figure 1 - Framework items showing interactions between causes of risky behaviours



The extent of the influence of risky behaviours is affected by the physical environment and situational factors. Physical environmental factors that can increase the likelihood and impact of risky behaviours include shared office spaces, lack of private meeting space and lack of turnstiles or controlled entry points. Situational factors that may affect behaviours include organisational performance, restructuring, redundancies, time-pressure and remote-working as a result of a pandemic. However, if an organisation had a good cyber security culture and secure ways of working, the impact of physical environment, or situational vulnerabilities, is likely to be smaller than if they had a poor cyber security culture. Similarly, a poor culture could affect investment in cyber security; time allowed for training; prioritisation of training; and likelihood of equipment misuse for example.

Transforming an organisational culture can be time-consuming and expensive. However, by addressing ways of working, the culture can start to mature. Conversely, if ways of working prove to be difficult to change, it may be necessary to examine the impact of the overall organisational culture.

3.4.3 Solutions in the framework reference tables

In Table 1, Table 2 and Table 3, mitigating recommendations are presented in terms of 'quick wins' and 'long-term solutions'. Quick wins indicate relatively inexpensive or short-term solutions. Some quick wins can be applied with off-the-shelf purchases (e.g., password managers), and others may require a small amount of in-house or consultancy HF expertise (e.g. designing specific cyber security information-sharing procedures around job needs). Long-term solutions may require a greater amount of time or resources to implement but are likely to have larger, longer-lasting effects than the quick wins. They pertain to culture change; job evaluation and re-design; working environments; resources and equipment.

3.5 How to use the framework

The framework tables (Table 1, Table 2 and Table 3) are intended to serve as a reference. As illustrated in Figure 2, the tables describe the causes of, and solutions to, specified risky behaviours that can affect the cyber security of organisations. Organisational causes are categorised by culture, ways of working, situational factors and physical environment factors. Some of the causes apply to several risky behaviours. These are truncated in the main table (Table 1) to avoid repetition, and presented in more detail in Table 2 and Table 3. Table 2 addresses common organisational causes, and Table 3, individual causes.

The behaviours in the tables can be incorporated into data collection materials (e.g. questionnaires, interview and focus group templates) to capture HF-related cyber security issues. Documentation, such as policies and job descriptions, are also useful sources of data. Similarly, observation and monitoring can be used to assess some of the behaviours.

Data collection results can be used to identify the organisational cyber security maturity level. Table 4 presents HF considerations mapped to cyber security maturity levels. The tabulated framework solutions (in Table 1, Table 2 and Table 3) can be consulted to enhance cyber security and raise the maturity level. An organisational change process, such as the '4E's (Enable, Encourage, Engage and Exemplify) policy framework[34], can be implemented to advance the issues, identified during data collection, towards the desired state captured in the recommendations.

The framework can also be used retrospectively, as a checklist to identify factors that may have contributed to cyber security incidents.

[34] Cabinet Office, Institute for Governement, Mindspace. Influencing behaviour through public policy: https://www.instituteforgovernment.org.uk/sites/default/files/publications/MINDSPACE.pdf

Figure 2 – How to use the framework tables

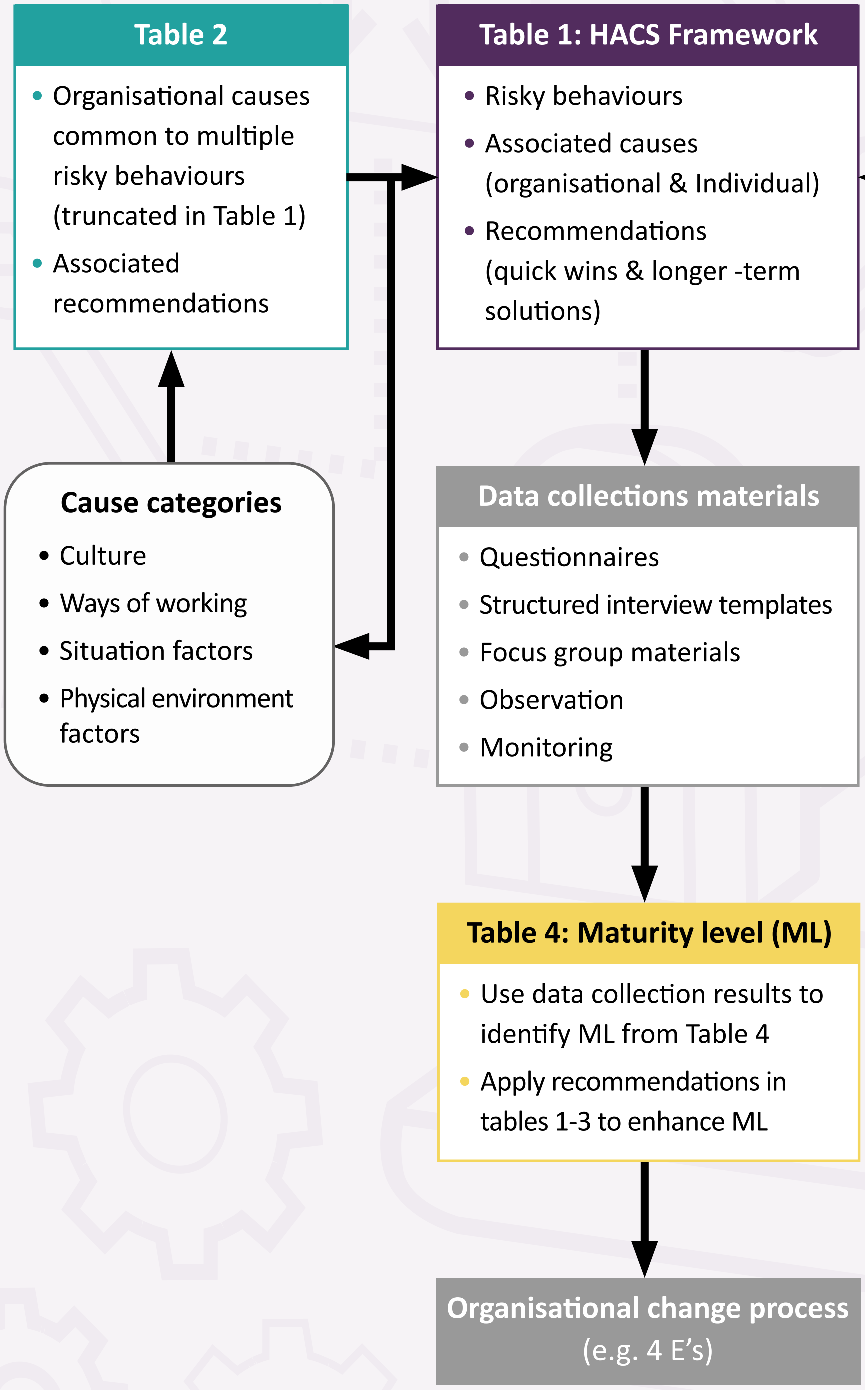


Table 2

- Organisational causes common to multiple risky behaviours (truncated in Table 1)
- Associated recommendations

Table 1: HACS Framework

- Risky behaviours
- Associated causes (organisational & Individual)
- Recommendations (quick wins & longer -term solutions)

Table 3

- Individual causes common to multiple risky behaviours (truncated in Table 1)
- Associated recommendations

Cause categories

- Culture
- Ways of working
- Situation factors
- Physical environment factors

Data collections materials

- Questionnaires
- Structured interview templates
- Focus group materials
- Observation
- Monitoring

Table 4: Maturity level (ML)

- Use data collection results to identify ML from Table 4
- Apply recommendations in tables 1-3 to enhance ML

Organisational change process
(e.g. 4 E's)

Table 1 – Human Affected Cyber Security (HACS) framework

#	Risky behaviours	Organisational causes	Individual causes	Quick wins	Long-term solutions
1	**User validation violations**				
1.1	Create passwords that are easy to guess.	*Ways of working* Inappropriate password policies - asking people to change passwords frequently. No restrictions in place to ensure the creation of sufficiently complex passwords. Password managers not supplied or encouraged.	Human memory capacity - multiple personal & professional applications requiring passwords. Lack of knowledge of risk (see common causes).	Password safes/ managers.	Alternatives to passwords (e.g., biodata - fingerprint, facial recognition, etc.)
1.2	Use the same password for multiple applications (personal and professional).	*Ways of working* Inappropriate password policies - asking people to change passwords frequently. Password managers not supplied or encouraged.	Human memory capacity - multiple personal & professional applications requiring passwords. Lack of knowledge of risk (see common causes).	Password safes/ managers. Software should not necessitate frequent password changes.	Alternatives to passwords (e.g., biodata - fingerprint, facial recognition, etc.)
1.3	Share password/ login details with other(s).	*Ways of working* Job/system requires people to use the same accounts/ passwords. Password managers not supplied or encouraged. *Culture* Norm for cyber security cyber security to be low priority.	Lack of knowledge of risk (see common causes). Over trust in colleagues.	Password safes/ managers.	Investigate job/ equipment design to identify cause. Alternatives to passwords (e.g., biodata - fingerprint, facial recognition etc.). Implement recommendations from CSMA), incorporating the behaviours in this framework, as part of continuous improvement activities.
1.4	Write password down in unsafe place.	*Ways of working* Poor job design/ technology solution. *Culture* Norm for cyber security to be low priority.	Human memory capacity - multiple personal & professional applications requiring passwords; Lack of awareness of risk (see common causes).	Password safes/ managers.	Alternatives to passwords (e.g. biodata - fingerprint, facial recognition, etc.). Implement recommendations from CSMA, incorporating the behaviours in this framework, as part of continuous improvement activities.

#	Risky behaviours	Organisational causes	Individual causes	Quick wins	Long-term solutions
2	**Information sharing**				
2.1	Wear lanyards or clothing, that identifies employer, in public.	*Ways of working* Clothing and lanyards purchased and encouraged, without a policy to limit use to work environments. *Culture* Common to wear company branded clothing in public without concern for security implications so it becomes a norm.	Human memory capacity – people will forget they are wearing signifiers. Lack of knowledge of risk (see common causes). Personality (see common causes).	Posters at exits reminding people to remove signifiers when not in the workplace. Ask employees not to identify themselves as being part of the organisation in public. Managers openly conform to the policy.	Implement recommendations from CSMA, incorporating the behaviours in this framework, as part of continuous improvement activities.
2.2	Talk about sensitive information in public areas (e.g., pub, coffee shop) or other areas where unauthorised individuals may be present.	*Physical environment* Shared buildings/ office space/ facilities make it easier for unauthorised individuals to access or overhear sensitive information. Insufficient number of breakout rooms to discuss sensitive information privately. *Culture* Cyber security routinely not considered in public/shared areas. *Situational factors* Remote working may inadvertently blur the lines between work and home life.	Lack of knowledge of risk (see common causes). Personality (see common causes). Employee(s) feels unappreciated, e.g. passed over for promotion, lack of reward/recognition and a change to personal circumstances (malicious or seeking support).	Ask employees not to identify themselves as being part of the organisation in public. Managers careful not to speak about sensitive information in public areas. Encourage all employees to intervene when they hear sensitive information discussed in public areas.	Implement recommendations from CSMA, incorporating the behaviours in this framework, as part of continuous improvement activities.

Table 1 – Human Affected Cyber Security (HACS) framework (continued)

#	Risky behaviours	Organisational causes	Individual causes	Quick wins	Long-term solutions
2	**Information sharing**				
2.3	Use personal email account to share information.	*Ways of working* Company information sharing policies and software restrictions prevent legitimate information sharing. *Culture* Organisational culture values performance over security. *Situational factors* Remote working may inadvertently blur the lines between work and home life.	Lack of knowledge of risk (see common causes). Personality (see common causes).	Design cyber security information-sharing procedures around job needs.	Investigate job/ equipment design and organisational culture to identify cause.
2.4	Send sensitive information (e.g. login details, passwords, personal details) over email, to unknown or unauthorised accounts.	*Ways of working* Company information sharing policies prevent legitimate information sharing. Lack of training provision. *Culture* Performance/ productivity is valued over cyber security.	Lack of knowledge of risk (see common causes). Personality (see common causes).		Invest in equipment to detect malicious emails and sharing of sensitive information.
2.5	Share sensitive information on video-conferencing platforms.	*Ways of working* Company information sharing policies prevent legitimate information sharing. *Culture* Performance/ productivity is valued over cyber security. Use of video-conferencing encouraged.	Lack of knowledge of risk (see common causes). Personality (see common causes).	Design cyber security information-sharing procedures around job needs. Provide training.	Investigate job/ equipment design and organisational culture to identify cause.

#	Risky behaviours	Organisational causes	Individual causes	Quick wins	Long-term solutions
2	**Information sharing**				
2.6	Share sensitive information/ complain about employer on social media.	*Ways of working* No policy/training in place to make it clear what can be shared on social media. *Culture* Environment where employees are not made to feel valued or supported. *Situational factors* Employee(s) made to feel unappreciated, e.g. lack of promotion opportunities, lack of reward/ recognition and threat of redundancies. Remote working makes it more difficult to monitor emotional wellbeing of employees.	Lack of knowledge of risk (see common causes). Personality (see common causes). Employee(s) feels unappreciated, e.g. passed over for promotion, lack of reward/recognition and a change to personal circumstances (malicious insider attack or seeking support).	Managers and colleagues to identify and report malicious behaviours. Consider blocking social media from work devices. Provide training.	Monitor company information on social media (open source intelligence).
3	**Misuse of technology**				
3.1	Use compromised or unsafe equipment (e.g., USB, unauthorised printer, unprotected personal email).	*Ways of working* Company information sharing policies prevent legitimate information sharing. *Culture* Performance/ productivity is valued over cyber security.	Lack of knowledge of risk (see common causes). Personality (see common causes). Over-trust in IT department to protect them – lack of ownership for cyber security.	Design cyber security information-sharing procedures around job needs.	Implement peripheral equipment access management controls. Implement recommendations from CSMA, incorporating behaviours from this framework, as part of continuous assessment activities.

Table 1 – Human Affected Cyber Security (HACS) framework (continued)

#	Risky behaviours	Organisational causes	Individual causes	Quick wins	Long-term solutions
3	**Misuse of technology**				
3.2	Click email links and download attachments from unknown email addresses.	*Ways of working* Lack of time (time pressure) causes victim to read and react quickly with little attention. Poor email management/ excessive emails. Difficult to tell email is from external source. Insufficient anti-virus protection. *Culture* Performance/ productivity is valued over cyber security.	Personality (see common causes). Unable to detect phishing/whaling email or social engineering-based attacks. Unaware of indicators and risks. Over-trust in IT department to protect them – lack of ownership for cyber security.	emails for manual check. Provide alert indicating the email is from an external source.	incorporating behaviours from this framework, as part of continuous assessment activities.
3.3	Inappropriate internet and email usage.	*Ways of working* Inadequate whitelist. Job requires access to 'at-risk' websites. Inadequate anti-malware. *Culture* Performance/ productivity is valued over cyber security. Norm for cyber security to be low priority. Perception of inadequate monitoring.	Lack of knowledge of risk (see common causes). Personality (see common causes). Use work computer or email account for non-work activities.	Consider blocking unknown websites. Overtly monitor internet and email use Add anti-malware software. Provide training.	Conduct job analysis to determine sites that are needed to enable normal work, or introduce a process for sites to be checked and added to a whitelist.

#	Risky behaviours	Organisational causes	Individual causes	Quick wins	Long-term solutions
3	**Misuse of technology**				
3.4	Download unknown software or updates	*Ways of working* Inadequate technology measures in place. Job requires access to the software packages before approval. Inadequate administrative controls. *Culture* Performance/ productivity is valued over cyber security. Norm for cyber security to be low priority.	Lack of knowledge of risk (see common causes). Personality (see common causes). Use computer for non-work activities. Over-trust in IT department to protect them – lack of ownership for cyber security.	Implement useable administrative process to prevent download of unapproved software.	Invest in automatic detection and prevention of unapproved software. Implement recommendations from CSMA, incorporating behaviours from this framework, as part of continuous assessment activities.
3.5	Fail to install updates and patches	*Ways of working* Inadequate asset management. *Culture* Lack of investment in cyber security resilience and IT infrastructure. Lack of investment in trained Information Security personnel.	Memory/ attentional failure.		Invest in an asset management system and training for Information Security personnel (or equivalent accountable employees).
3.6	Use of public Wi-Fi	*Ways of working* IT Acceptable Use/ cyber security policy does not restrict the use of public Wi-Fi. There are no safe workable alternatives (e.g. mobile data) and the job requires online access in public locations. *Culture* Performance/ productivity is valued over cyber security. Physical environment Insufficient office space encourages employees to use public spaces.	Lack of knowledge of risk (see common causes). Personality (see common causes). Use computer for non-work activities.	Provide mobile data to employees for securely connecting in public places. Enforce the use of Virtual Private Networks (VPN).	Conduct job analysis to determine when, where and why public Wi-Fi is being used, and use the results to make organisation-level changes.

Table 1 – Human Affected Cyber Security (HACS) framework (continued)

#	Risky behaviours	Organisational causes	Individual causes	Quick wins	Long-term solutions
4	**Training**				
4.1	Employees do not complete cybersecurity training.	*Ways of working* Training inaccessible or difficult to find. Training not mandated or monitored. Training activities not included during on-boarding. Training poorly designed, lacking relevance. *Culture* Managers do not exhibit good cyber security behaviours (‘walk the talk’). Lack of time allowed for training.	Unaware of training.	Provide accessible cyber security training (see common causes). Managers to encourage and monitor training. Introduce good quality, meaningful, and relevant mandated training. Add training to on-boarding activities.	Create a culture where cyber security is valued and discussed openly. Produce and maintain a competence management system so are aware of who has had training when and to what competence standard.
4.2	Employees do not take ownership of cyber security/ negative attitude towards cyber security.	*Ways of working* Employees are not asked to take responsibility for cyber security. *Culture* Managers and peers do not exhibit good cyber security behaviours (‘walk the talk’). Cyber security policy/procedures not endorsed by senior managers.	Over trust in IT department to protect them. Lack of knowledge of risk (see common causes). Personality (see common causes).		Encourage ownership of cyber security, get employees involved in protecting organisation.
5	**Poor monitoring and incident management**				
5.1	Incidents not reported.	*Ways of working* No process for reporting incidents. No system to make it easy to report incidents. *Culture* Fear of consequences e.g., reputational damage; blame/ punishment.	Fear that reporting an incident will incur blame and punishment. Personality (see common causes).	No punishment for incidents. Accessible incident-reporting system.	Open policy about incident sharing with lessons learnt shared. Create ‘Just Culture’.

#	Risky behaviours	Organisational causes	Individual causes	Quick wins	Long-term solutions
5	**Poor monitoring and incident management**				
5.2	Incidents/near misses not recorded.	*Ways of working* Lack of time allowed for cyber security; lack of ownership for incident management. Onerous incident-reporting process. *Culture* Managers do not exhibit good cyber security behaviours ('walk the talk'). Blame and punishment attributed when incidents are reported.	Fear that reporting an incident will incur of blame and punishment.	Record incidents and near misses	Investigate and share lessons from internal and external incidents. Create 'Just Culture'.
5.3	Lessons not learnt.	*Ways of working* Incidents not investigated fully (lack of knowledge of root causes). Investigation results not shared. HF not considered in incident investigations, (lack of knowledge of benefits/role of HF practitioners in cyber security/ incident investigations). *Culture* Managers do not exhibit good cyber security behaviours ('walk the talk').	Unaware of lessons from previous incidents.	Implement governance to enable the organisation to monitor, anticipate, respond and learn from cyber security incidents. Routinely communicate lessons learnt e.g. at the start of new projects/meetings. Include HF expertise in incident investigation. Cyber security incident investigation and root cause analysis - consider a broad range of factors that could cause incident, including HF. Reward employees for reporting incidents/near misses.	Investigate and share lessons from internal and external incidents. Create 'Just Culture'.

Table 1 – Human Affected Cyber Security (HACS) framework (continued)

#	Risky behaviours	Organisational causes	Individual causes	Quick wins	Long-term solutions
5	**Poor monitoring and incident management**				
5.4	Failure to monitor employee behaviour relating to cyber security.	*Ways of working* No monitoring policies or processes in place. Line managers are not given responsibility for monitoring employee cyber security behaviours (may be seen as a Human Resources (HR) issue). *Culture* Managers do not exhibit good cyber security behaviours ('walk the talk').	Lack of knowledge of risk (see common causes).	Introduce monitoring processes as part of line manager responsibilities.	Introduce automated monitoring and anomaly detection systems. Create a culture where cyber security is valued and discussed openly.
5.5	Failings in response to an attack (e.g. slow to respond).	*Ways of working* No procedures in place for how to respond to an attack. No procedures in place for how to recover following an attack.	Lack of awareness of attack. Lack of knowledge of the risk (see common causes). Incorrect attribution of incidents to non-malicious causes (e.g. poor IT maintenance or mechanical failure).	Create emergency operating procedures in case of an attack. Procure cyber security incident response services from a third party in advance of an incident. HF design of Information Security (IS) information.	Establish in house Cyber Security Operations Centre (CSOC).
5.6	Lost devices/old accounts not reported.	*Ways of working* Lack of usable reporting process/tool. *Culture* Blame and punishment attributed when incidents are reported. Relaxed attitude to loss of information. *Situational factors* Remote working and need for travel increase the likelihood of lost equipment/documents.	Personality (see common causes).	Implement and police usable procedures to report lost devices and close old accounts. Audit assets and accounts.	Invest in asset management system. Create 'Just Culture'.

#	Risky behaviours	Organisational causes	Individual causes	Quick wins	Long-term solutions
6	**Neglecting physical environment security**				
6.1	Hold doors open for unauthorised individuals/allow tailgating.	*Physical environment* No access controls or turnstiles in place. Office/building shared with other organisations. *Ways of working* Poor visitor management policy. Nobody explicitly responsible for security (diffusion of responsibility). *Culture* Building security not prioritised as part of cyber security.	Lack of knowledge of risk (see common causes). Personality (see common causes). Politeness - embarrassment prevents asking for credentials.	Warning signs on doors. Intermittent uniformed security presence to eliminate diffusion of responsibility.	Turnstiles with identification entry.
6.2	Fail to challenge someone who has gained unauthorised access to building.	*Physical environment* Office/building shared with other organisations. *Ways of working* Poor visitor management policy. *Culture* It is the norm to see unfamiliar personnel in the workspace.	Politeness. Personality (see common causes).	Good visitor management policy so it is clear who is a visitor and whether they should be escorted. Use identity cards/ badges to make it easier to identify unauthorised personnel.	Designate physical security responsibility to named personnel to reduce bystander apathy and concern about politeness.
6.3	Fail to wear lanyard inside where required (to denote access approvals).	*Ways of working* Lanyards or visible identification information, to distinguish employees and visitors, not supplied or used. *Culture* Failure to wear lanyards/identity information is not challenged and becomes the norm.	Lack of knowledge of risk (see common causes). Personality (see common causes).	Communicate the need to wear appropriate lanyard. Managers demonstrate lanyard wearing and challenge those who don't wear one.	

Table 1 – Human Affected Cyber Security (HACS) framework (continued)

#	Risky behaviours	Organisational causes	Individual causes	Quick wins	Long-term solutions
6	**Neglecting physical environment security**				
6.4	Leave sensitive content visible and accessible (fail to lock computer screen) when not at desk.	*Ways of working* Locking of computer screens not monitored/ policed. *Culture* Leaving computer screens unlocked is the norm.	Lack of knowledge of risk (see common causes). Personality (see common causes).	Communicate need to lock computer screens when not at desk and police this. Provide privacy filters for monitors.	Create a cyber security aware environment where employees would encourage each other to lock screens when they are not at desks.
6.5	Fail to secure server/network/ storage room	*Physical environment* Open or shared access. Key kept in open location. *Ways of working* Many people with regular access. No access log.	Lack of knowledge of risk (see common causes). Personality (see common causes).	Reduce number of people with access. Keep access log.	Provide automated pass-entry system for server/ network/storage areas.
6.6	Leave sensitive information on desks and printers.	*Physical environment* Lack of lockable storage. Shared equipment. *Ways of working* No clear-desk policy/clear desk policy not policed. Process for collecting paperwork at the printer takes longer than remote printing. *Culture* Leaving documents on accessible spaces, such as desks/printers, is the norm.	Lack of knowledge of risk. Memory/ attentional failure. Personality (see common causes).	Provide adequate lockable storage. Clear desk/ whiteboards policy.	Invest in private office space and facilities. Encourage all employees to play an active role in cyber security. Provide printers that require the sender's presence at the machine before releasing documents. Ensure the process for document release is quick and requires the minimal number of steps.
6.7	Fail to securely dispose of confidential documents.	*Ways of working* No process for appropriately disposing of documents. Lack of equipment for disposing of documents. *Culture* Failure to dispose of documents securely is the norm.	Lack of knowledge of risk (see common causes).	Introduce a process to include registering the printing, storing and disposal of confidential documents. Provide shredder. Procure services of certified suppliers to dispose of documents.	

#	Risky behaviours	Organisational causes	Individual causes	Quick wins	Long-term solutions
7	**Deliberate, malicious insider attack**				
7.1	Deliberate, malicious insider attack.	*Situational factors* Employee(s) made to feel unappreciated, e.g. passed over for promotion, lack of reward/ recognition, threat of redundancies. Remote working caused by pandemic makes it more difficult to monitor emotional wellbeing of employees. Ways of working Unpopular company policies. Failure to provide adequate emotional support to employees. Matrix management structures can result in shared responsibility for duty of care. May be seen as an HR issue and line managers and team-members do not take responsibility for monitoring cyber security behaviours. Remote working policy makes it more difficult to monitor emotional wellbeing of employees. Individuals have access to large amounts of sensitive information. *Culture* Environment where employees are not made to feel valued or supported.	Personal circumstances can affect employee emotional wellbeing. Personal circumstances increase vulnerability to blackmail. Exploitable beliefs. Boredom/desire for fun. Personality (see common causes).	Understand their duty of care. Provide time for team building events and coffee chats. Introduce monitoring processes as part of line manager responsibilities. Conduct additional personal checks before appointing people to security critical roles.	Introduce easy and anonymous mechanism for reporting employee wellbeing issues. Limit the amount of sensitive information accessible by individuals, e.g. split access to sensitive information between different people

Table 2 - Organisational causes common to multiple risky behaviours, with solutions[35]

Organisational causes	Quick wins	Longer-term solutions
Performance/productivity is valued and/or rewarded more than good cyber security behaviour.	Encourage, promote and reward good cyber security behaviours (e.g. number of potential incidents prevented).	
Lack of rewards/recognition for good cyber security behaviours.		Invest in reward/recognition for good cyber security behaviours.
Lack of time allowed for cyber security.		Allow adequate time for cyber security controls, including training and information management. Communicate consequences to senior management if insufficient time is allowed.
Poor cyber security behaviours/**lack of compliance is considered the norm.**	Encourage employees to challenge poor cyber security behaviours.	Implement recommendations from Cyber Security Maturity Assessment (CSMA), incorporating the behaviours in this framework, as part of continuous improvement activities. Strive for a 'Just Culture'[36]. Consider the maturity level indicators in Table 4 and implement a change process to increase maturity, for example applying the 4E's (Enable, Encourage, Engage and Exemplify) policy framework[37].
Managers do not exhibit good cyber security behaviours ('walk the talk').	Managers exhibit good cyber security behaviours, e.g. talk openly about expectations in regard to cyber security, give adequate priority and time to cyber security in balance with productivity, follow process without workarounds. Senior Manager(s) to endorse cyber security /information management policies. This helps create a positive cyber security culture.	

[35] Additional, specific causes and solutions are in Table 1.

[36] Renaud, K., & Dupuis, M. (2019, September). Cyber security fear appeals: Unexpectedly complicated. In Proceedings of the New Security Paradigms Workshop (pp. 42-56).

[37] Cabinet Office, Institute for Governement, Mindspace. Influencing behaviour through public policy: https://www.instituteforgovernment.org.uk/sites/default/files/publications/MINDSPACE.pdf

Organisational causes	Quick wins	Longer-term solutions
Lack of investment in cyber security and resilience.		Invest in cyber security: Invest in training (for employees and Information Security personnel). Conduct threat anticipation and monitoring, incident response planning and (HF) incident investigation, for example following Hollnagel's Resilience Analysis Grid[38]. Invest in equipment and operating systems. Invest in reward systems for good cyber security behaviours. Apply a governance model such as the 'Three Lines of Defence'[39]. The first line is focused on assigning ownership and accountability for mitigating risk. The second line advocates a risk management and compliance function that facilitates and monitors effective risk management practices. The third line refers to an internal audit function that provides the board with competent and objective assurance on how the organization is assessing and managing risk. Apply the HF Cyber Security Framework (Table 1) as part of the risk assessment and audit process. Apply HF presentation of information principles[40] to enhance the design of cyber security risk reporting for the board and cyber security stakeholders.
Insufficient management and monitoring of **contractors & suppliers.**	Apply HF principles adopted for permanent employees. Conduct thorough screening and monitoring of contractors and suppliers. Restrict supplier access to critical systems. Provide/ensure adequate training for suppliers with access to systems.	Specify cyber security requirements in supplier contracts.

[38] https://erikhollnagel.com/ideas/resilience%20assessment%20grid.html Copyright © Erik Hollnagel 2016 All Rights Reserved.

[39] Deloitte. Cybersecurity: The changing role of audit committee and internal audit. Available from https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cybersecurity-the-changing-role.pdf

[40] IS9241-112, Ergonomics of Human System Interaction, 2017, Principles for the Presentation of Information

Table 3 – Individual causes common to multiple risky behaviours, with solutions[41]

Individual causes	Quick wins	Longer-term solutions
Personality: Some personality types are more vulnerable (e.g. high social compliance, highly trusting, low straightforwardness, sense of duty, conscientiousness).	Using a qualified professional, conduct psychometric personality profiling for security critical roles (i.e. those with frequent access to highly sensitive information/ controls). This can support recruitment but should also be considered for longer-serving employees and those with significant access to sensitive information and/or cyber security controls.	
Lack of knowledge of cyber threats and vulnerabilities and how they impact them (partially individual but likely to be caused by inadequate training provision; lack of refresher training; poor competence management system *(Organisational).*	Provide, accessible cyber security training to include attack examples relevant to the target audience, phishing email management, visitor management and measurement of competence; a test. Create a sense of urgency but provide solutions to build confidence in ability to cope.	Produce and maintain a competence management system to sustain awareness of who has had training when and to what competence standard.
	Openly share threat and key incident information amongst employees and similar organisations.	Create and manage incident database.
		Conduct cyber security risk assessments and include consideration of HF (for example, using Table 1).

[41] Additional, specific causes and solutions are in Table 1.

HF considerations are mapped to cyber security maturity levels in Table 4. Once the organisational maturity level has been identified, a change process can be implemented to increase maturity, as described in Section 3.6.

Table 4 - HF considerations mapped to NIST[42] maturity levels

Maturity Level	Name	General Description
LEVEL 1	Reactive	• Cyber security/information management processes are not formalised. • Inconsistent execution of cyber security processes. • Focus on compliance with standards only. • Many cyber security incidents (including poor behaviours) are seen as unavoidable. • Most front-line staff are uninterested in/unaware of cyber security. • Minimal cyber security incident sharing. • Information Security (IS) function lacks competence and is poorly co-ordinated across organisation. • No appointed Chief Information Security Officer (CISO) or CISO reports to a manager in IT department. • Minimal reporting.
LEVEL 2	Repeatable	• Process is more formalised (documented). • Repeatable execution of processes. • Management understands overall process. • Cyber security incident rate average but incidents/behaviours more serious than average. • Managers perceive accidents are caused by poor behaviours of frontline staff. • Senior managers are reactive. • Senior managers aware of cyber security threats. • Performance measured in terms of lagging (retrospective) indicators (instead of number of control measures). • CISO reports to Chief Operating Officer (COO)/non-IT senior manager. • Reporting only focusses on measurement of activity (such as completion rates) rather than effectiveness and impact on risk.

[42] NIST (2014), Framework for Improving Critical Infrastructure Cybersecurity - Version 1.0, National Institute of Standards and Technology February 12, 2014

Maturity Level	Name	General Description
LEVEL 3	Defined and Managed	• Process is fully defined and executed consistently. • Adequate metrics are defined to allow for quality assurance/self-assessment capabilities. • Managers promote cyber security risk and control knowledge. • CISO reports to Chief Executive Officer (CEO). • Formal cyber security training conducted and includes a measure to test understanding. • Majority of staff believe cyber security is important. • Managers recognise cyber security incidents/behaviours are likely to have root causes in management decisions (a just and fair culture). • Majority of staff aware of cyber security risks and accept responsibility for own and others’ cyber security. • Importance of all employees feeling valued and treated fairly is recognised. • Significant proactive effort (e.g. Cyber Vulnerability Investigations (CVI)/risk assessments). • Cyber security performance measured using all data available (including HF and incident monitoring). • Regular training exercises (role play). • Formal cyber security incident sharing. • Automated behavioural analytics. • Managers tackle significant cyber security incidents without delay. • Managers recognise good cyber security behaviours and address poor cyber security behaviours and performance
LEVEL 4	Sustained	• Management decision-making and continuous improvement projects are based on data, metrics, and formal quality assurance/self-assessment feedback. • Years without a recordable/high potential cyber security incident/behaviour but not complacent. • Range of indicators to monitor cyber security performance (but not performance-driven). • Employees are confident in cyber security processes. • Constantly striving to do better in cyber security and improve controls. • All employees believe cyber security is critical to their job and accept prevention of cyber security incidents is important.
LEVEL 5	Optimised	• Optimal service levels are achieved. • Independently verified as best-in-class. • Innovative ideas and techniques are piloted on an ongoing basis. • Prevention of cyber security incidents (at work and home) is a core company value and the company invests significant effort to promote it. • There is considerable effort given to measuring “success” through improvement and evaluation. Baseline measurements are taken prior to implementation of interventions, and data is analysed post-implementation to identify impact.

4.0 Summary

Cyber security incidents can cause significant disruption, financial and reputational damage to individuals and organisations. As described in section 2.0, the human element is acknowledged as a causal factor in such incidents.

In cyber security, the use of prescribed levels of physical security, network security, point of use security, application security and data security, are all bounded by standard/emergency operating procedures and policy. They are becoming essential components of an overall formalised strategy. However, it is not always clear where the human is considered in such a strategy. Humans have long been a key component in sociotechnical systems, such as oil refineries, nuclear power stations or military battle spaces, and are the keystone to organisational integrity and safety assurance. Lessons learned from HF support to safety and incident investigation, can be applied to enhance cyber security. With the rise of cyber-attacks that circumvent technical defences, the best (and only) defence is, arguably, a human. Human flexibility, situation appreciation and decision-making are strong defences against such attacks and phishing attempts.

The Human Affected Cyber Security (HACS) Framework presents lower level, specified, undesirable behaviours and associated solutions. It can be used proactively, to assess and mitigate cyber security risks, and retrospectively, to identify potential human-related incident causes. The framework includes categorised risky behaviours. Incorporated causes pertain to organisational culture, ways of working, situational factors and the influence of the physical environment. A smaller group of individual causes; factors associated with individual people, are also presented. However, the recommended solutions largely pertain to changes at a system or organisational level. By addressing these systemic, organisational failures, the risk of human-related cyber security incidents can be reduced.

5.0 Authors, contributors and reviewers

5.1 Authors and contributors

- Amanda Widdowson, CIEHF President 2020/21, Head of Human Factors Capability, Thales UK
- Nicola Turner, Senior Human Factors Scientist, Trimetis, UK
- Dr John Blythe, Director of Cyber Workforce Psychology, Immersive Labs, UK
- Alessandra Tedeschi, R&D Director, Deep Blue srl, Italy
- Andrea Capaccioli, Senior Consultant, Deep Blue srl, Italy
- Owen Marsh, Abbott Risk Consulting
- Robert Williams, Abbot Risk Consulting, UK
- Dr Eylem Thron, Principal Consultant, Mima, UK

5.2 Reviewers

- Simon Pavitt, Head of Cyber Awareness, Behaviours & Culture, Ministry of Defence, UK
- Professor Phillip Morgan, Chair in Human Factors and Cognitive Science & Director of the Human Factors Excellence Research Group (HuFEx), School of Psychology, Cardiff University UK; Director of Research – Cardiff University Centre for AI, Robotics and Human-Machine Systems (IROHMS); Technical Lead in Cyberpsychology and Human Factors, Airbus, Newport, UK.
- Andrew Wright, CRA-Assystem
- Dr Dennis Desmond, PhD, University of the Sunshine Coast, Australia
- Matt Barron, Human Factors Principal Consultant, Abbott Risk Consulting, UK
- CIEHF Council members, with special thanks to Alex Stedmon, Jon Berman, Robert Bridger and Terry Lansdown

Published 16 March 2022
Amendments made to this page 21 March 2022

Chartered Institute
of Ergonomics
& Human Factors

www.ergonomics.org.uk
ciehf@ergonomics.org.uk

Designed for CIEHF by Connect Communications – connectmedia.cc

The Chartered Institute of Ergonomics & Human Factors (CIEHF) received its Royal Charter in 2014 to recognise the uniqueness and value of the scientific discipline and the pre-eminent role of the Institute in representing both the discipline and the profession in the UK. This includes the protected status of "Chartered Ergonomist and Human Factors Specialist" with the post-nominal C.ErgHF awarded to practising Registered Members/Fellows who are among a group of elite professionals working at a world-class level.