Chartered Institute
of Ergonomics
& Human Factors

The role of human factors in delivering cyber security

An overview for cyber security decision-makers

WHITE PAPER

#ciehf


elif
mirror
bpy.context.scene.objects
print("Selected

Executive Summary

Many cyber security incidents have been attributed to a human element. However, it is also important to recognise that human flexibility, situational awareness, and decision-making can strengthen cyber security and although defences are engineered, their integrity is human mediated. This paper provides a summary of what the discipline of human factors (HF) brings to cyber security and promotes the adoption of a holistic systems perspective, taking account of the people within an organisation. It aims to give an understanding of HF cyber security considerations for policy makers, executives, chief information security officers (CISOs) and security practitioners. It is designed to help organisational decision makers to incorporate HF considerations into cyber security and to signpost when professional HF support may be helpful.

HF professionals apply an understanding of human strengths and limitations to identify and mitigate the risk of cyber security incidents within a system or organisation. This paper describes a selection of HF cyber security considerations, including behaviour change, cyber security maturity levels, organisational resilience, board decision-making, and presentation of cyber security information. Key recommendations have been highlighted at the end of each subsection to provide summarised guidance.

1. Behaviour change

This section describes a method for diagnosing the drivers behind positive (and negative) cyber security behaviours. By considering the capability, opportunity and motivation people have for engaging in a certain behaviour, interventions can be targeted and more effective.

2. Cyber security maturity levels

This section outlines a maturity model that addresses human, organisational and technical aspects. It can be used to help organisations assess their control and process management and identify the actions necessary to improve the maturity of the organisation, or process, using a systematic basis of measurement.

3. Organisational resilience

Organisations need to have appropriate systems in place to ensure they have the resilience to withstand a cyber security threat or event and recover quickly with minimal effect on its everyday business activities. This involves monitoring, anticipating, responding to, and learning from cyber security threats and incidents.

4. Board decision-making

Many boards feel ill-equipped to deal with cyber security challenges. Several barriers have been identified, such as time constraints, lack of dedicated budget for their cyber security strategy, differing reporting structures and inadequate reporting.

5. Presentation of cyber security information

Three critical success factors are identifying information needs, understanding how people perceive information, including decision-making bias, and usability testing of human decision-making performance.

Cyber security incidents can cause significant disruption, financial and reputational damage to individuals and organisations. The human element is acknowledged as a factor in such incidents but is rarely the root cause. Instead, the root cause is often a systemic, organisational failure that unless addressed will continue to influence organisational cyber security performance. The Human Affected Cyber Security (HACS) Framework has also been developed alongside this paper, it presents lower level, specified, undesirable behaviours and associated solutions. It was designed to be used by HF professionals and can be used proactively to assess and mitigate cyber security risks, and retrospectively, to identify potential human-related incident causes.

Contents

Executive Summary **3**
1.0 Introduction **5**
1.1 Who should read this paper? 5
1.2 Structure of paper 5
2.0 Problem definition: why do we need to consider HF in cyber security? **7**
2.1 What is a cyber security incident? 7
2.1.1 What are the costs? 7
2.2 Human factors - related causes of cyber security incidents 8
2.2.1 Three types of insider vulnerability 8
2.2.2 Summary of the need for HF in cyber security 12
3.0 HF Considerations **14**
3.1 Behaviour change 14
3.1.1 Behaviour change theory: the COM-B model 14
3.1.2 Theory to practice 15
3.2 Cyber security maturity models 16
3.2.1 Key recommendations 18
3.3 Organisational resilience 18
3.3.1 Monitor and anticipate 20
3.3.2 Respond 22
3.3.3 Key recommendations 22
3.4 Board-level decision-making 23
3.4.1 Key recommendations 23
3.5 Presentation of cyber security information 24
3.5.1 Identifying information needs 24
3.5.2 Understanding what influences perception and decision-making bias 24
3.5.3 Usability testing 25
3.5.4 Key recommendations 25
4.0 Summary **26**
5.0 Authors, contributors, and reviewers **27**
5.1 Authors and contributors 27
5.2 Reviewers 27

1.0 Introduction

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 now known as "insider threat" (including behaviours that are unintentional, intentional but non-malicious, or intentional and malicious). However, 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 and although defences are engineered, their integrity is human mediated. This paper provides human factors (HF) advice to enhance cyber security and promotes the adoption of a holistic systems perspective, taking account of the people within an organisation.

1.1 Who should read this paper?

This paper is designed to support organisational decision makers and its aim is to provide guidance on incorporating HF considerations into cyber security and to signpost when professional HF support may be helpful. It aims to give an understanding of HF considerations to policy makers, executives, chief information security officers (CISOs), and other security practitioners. Whilst the content is mostly targeted at larger organisations, many of the considerations are also applicable to small and medium-sized enterprises (SMEs) with some adaption. Another paper (HACS Framework) was developed in conjunction with this one, aimed at HF professionals, and can be used alongside this one to support more detailed analyses.

1.2 Structure of paper

The paper is structured as follows:

- Section 2.0 defines the problem and describes why we need to consider HF in cyber security.

- Section 3.0 explores HF considerations to support people in organisations and reduce the likelihood of a cyber security incident. This includes:
  - Behaviour and culture transformation: a method for diagnosing the drivers behind positive (and negative) cyber security behaviours to support the selection of appropriate and effective behaviour change interventions.
  - Cyber security maturity levels: how cyber security maturity can be enhanced and measured.
  - Organisational resilience: how to monitor, anticipate, respond to, and learn from, a cyber security threat or incident.
  - Board level decision-making: how to incorporate cyber security into business strategy.
  - Presentation of cyber security information: how cognitive ergonomics (part of HF) can support the presentation of Information Security data.

- Section 4.0 provides a short summary.


SYSTEM
HACKED

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

2.1 What is a cyber security incident?

Cyber security is the practice of protecting systems, networks, and programs from attacks. Such attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. The UK National Cyber Security Centre (NCSC) defines a cyber security incident as a breach of a system's security policy to affect its integrity or availability and/or the unauthorised access or attempted access to a system or systems; in line with the Computer Misuse Act (1990)[1]. In general, types of activity that are commonly recognised by the NCSC as being breaches of a typical security policy are:

1. **Attempts to gain unauthorised access to a system and/or to data.**
2. **The unauthorised use of systems for the processing or storing of data.**
3. **Changes to a system's firmware, software, or hardware without the system owner's consent.**
4. **Malicious disruption and/or denial of service.**

Cyber security incidents can vary from accessing an individual's social media account by social engineering, to large scale malicious cyber-attacks on organisations or government institutions. Approximately 89% of cyber breaches are financially motivated and 8% are motivated by espionage with state sponsored attacks also being motivated financially in 6-16% of recorded breaches[2].

Initially, the main role of cyber security professionals was to protect information security (IS) infrastructure and data. The role was reactive in nature; when a threat appeared or a risk materialised, it was eliminated as quickly as possible. Therefore, deep technical knowledge of IS infrastructure was necessary. Today, cyber security needs to be proactive, to anticipate threats from third parties, cloud environments and mobile devices, for example. Global digitalisation, operational technology, and the internet of things (IoT) have opened a myriad of new opportunities that cyber criminals and hackers can, and do, exploit. Therefore, it is important for cyber security teams, organisations, and individuals to have a broad range of skills to navigate the environments and threats pertinent to them. In addition, with an increasingly common perception that cyber incidents are inevitable, anticipating what attackers are going to do before they do it is key. Organisations with the foresight and ability to think like attackers are the ones who will provide the most value[3].

2.1.1 What are the costs?

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[4]. 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.

[1]Legislation.gov.uk. 1990. Computer Misuse Act [online] Available at: http://www.legislation.gov.uk/ukpga/1990/18/section/3ZA
[2]Verizon 2021 Data Breach Investigations Report (2021 DBIR Results & Analysis | Verizon) 10 August 2021, 16:20
[3]Will humans be relevant in the future of cyber security | Deloitte
[4]https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

Losses can be attributed directly to the incident, as reputational damage, and recovery, and, in the UK, if personal data has been taken the organisation can also be fined for a General Data Protection Regulation (GDPR) breach, of which the maximum fine is £17.5 million or 4% of annual turnover (whichever is greater)[5].

In addition to financial losses to 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. Examples of cyber security incidents, along with HF elements, are presented in boxes 1-4.

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"; and IBM[6] 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. In 2019, a CybSafe analysis of cyber data indicated that 90% of cyber breaches were due to human error[7]. However, using the terms insider threat and human error can appear to put the blame on people and may distract from the systemic, organisational failures that are at the root of such incidents and the key to preventing them.

2.2.1 Three types of insider vulnerability

Systemic failures are often causes of human error and these can be traced to organisational elements such as unclear policies and procedures, and managerial practices[8];[9]. However, it is important to understand different types of human error to minimise the risk of occurrence. Building on Pollini et al (2021)[10], three types of insider threat are described in the follow paragraphs:

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

2.2.1.1 Unintentional, non-malicious insider threat

Rasmussen's (1983)[11] classic taxonomy of human error describes skill-based, rule-based, and knowledge-based behaviours. Skill-based behaviours happen during routine, familiar tasks, typically performed automatically, with little conscious thought. A slip or lapse error may result from distraction, inattention, or memory failure. Rule-based errors include incorrect application of rules or operating procedures, failure to apply the correct rules, or application of incorrect rules. For example, a rule appropriate for one situation may be incorrectly applied to a similar situation. Knowledge-based errors are caused by a lack of knowledge or experience in a situation, or a failure to apply existing knowledge to a new situation. Rule and knowledge-based errors are mistakes, decision-making failures. This model is still applied to safety assessments.

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 based on their known interests or work context. Slips and lapses can account for

[6]IBM X-Force Threat Intelligence Index 2021
[7]https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
[8]Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. Applied Ergonomics, 38(2), 143–154. https://doi.org/10.1016/j.apergo.2006.03.010
[9]Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & Security, 28(7), 509–520. https://doi.org/10.1016/j.cose.2009.04.006
[10]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.
[11]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.

loss of sensitive information in laptops or paperwork. Forgetting to update software is another example of an unintentional error.
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.
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 1 below.

BOX 1 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[12].

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[13]. The tendency to trust people that we like[14] 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®)[15]. It illustrates that even a system with strong technical controls can be overridden by human operators.

[12] https://news.sky.com/story/barclays-cyber-raid-arrests-over-stolen-1-3m-10433789 https://www.bbc.co.uk/news/uk-england-london-27146037
[13] Rosenbaum M.E, Blake R.R. (1955). Volunteering as a function of field structure *Journal of Abnormal and Social Psychology,* 50, pp 193-6.
[14] 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).
[15] 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 often performed in an attempt to get the job done in a more efficient manner, or due to other conflicting demands. If cyber security policy and procedures are too strict, employees may find workarounds. Beautement et al (2008) describe a "compliance budget"[16]; a cost-benefit analysis that results in people either choosing to not 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. 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)[17], culminating in risky security behaviours.

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 several 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[18]and sabotage[19].

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[20]. It is important to remember that people can change since any initial screening during recruitment. Susceptible employees may also 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 and external attacks can be initiated by individuals or highly organised crime organisations. Motivations could include political beliefs, state attacks, commercial espionage, or simply fun. An example attack that was motivated largely by fun, but with severe consequences, was incurred by the Polish tram system in 2008 (see box 2).

[16]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).
[17]Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security.
[18]Hadlington, L. J. (2018). Employees attitudes towards cyber security and risky online behaviours: an empirical assessment in the United Kingdom.
[19]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.
[20]Cohen, LE, Felson, M, 1979, "Social change and crime rate trends: A routing activity approach", American Sociological Review 44 (4): 588-608

BOX 2 POLISH TRAIN, 2008[21]

What happened?
A 14-year-old Polish student, hacked into the tram system which enabled him to change track points in Lodz, Poland in 2008.

Consequences
Four trams were derailed. Twelve people were injured when a train derailed. No deaths occurred. The boy faced a special juvenile court on charges of endangering public safety.

Causes
The teenager built an infrared device that looked like a TV remote control that could control all the junctions on the line. He was an IT student with good academic skills. He took keen interest in his 'Electronics' class and was considered a genius by his teachers. He became interested in railways after learning about them at school. He spent months studying the Lodz Tram System and often spent his leisure time trespassing at Tram Depots to gather information and equipment. He learned coding skills from open-source public libraries (Altaf et al. 2019[22]). According to online articles and incident records, he did not wish to intentionally cause harm. Instead, the attack was exploratory in nature with no consideration given to its consequences. Curiosity and passion were identified as the major motivation, and the attacker was equipped with no more than basic knowledge about the information and railway sector (Altaf et al. 2019). There were four major vulnerabilities identified in the Polish tram system, namely faulty track points, reported problems with signalling system, an outdated switching system, and a lack of risk assessment which could be exploited by the teenager with little effort (Altaf et al. 2019).

HF Lessons
This example showed that hacktivists or hobby hackers can cause considerable damage even though they do not intend harm. Curiosity or a desire to test skills, personal characteristics, daily routines, interests, socialisation, and scope of hacking can lead an attacker to hack into systems with little consideration of the consequences (Altaf et al. 2019). Therefore, a tailored, structured approach for security assessments and techniques is needed to understand such an attacker's motivations, skills, and capabilities. This could help security engineers to mitigate risks (Altaf et al. 2019)[23].

[21] https://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html
[22] Altaf, A., Abbas, H., Iqbal, F., & Derhab, A. (2019). Trust models of internet of smart things: A survey, open issues, and future directions. Journal of Network and Computer Applications, 137, 93-111.
[23] Altaf, A., Faily, S., Dogan, H., Mylonas, A. and Thron, E., 2019. Identifying safety and human factors issues in rail using IRIS and CAIRIS. In Computer Security (pp. 98-107). Springer, Cham.

2.2.2 Summary of the need for HF in cyber security

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.

Cyber Essentials (CE) is a UK Government backed scheme that aims to help organisations guard against common cyber threats. It provides an effective foundation to ensure certain measures are in place and offers some consideration of human factors. However, a deeper understanding of organisation vulnerabilities and causes of human error is important for knowing whether these measures are enough and what additional measures could be implemented.

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 current and future attacks. Therefore, greater consideration of HF is likely to enhance cyber security.

[24] https://www.ncsc.gov.uk/cyberessentials/overview


RTC32
1R2
C509
C501
C500
R35
IC105
C601
25.0F6K
SKW23
C-100
16V
RTC27
IC101
R32
C602

3.0 HF Considerations

The previous sections outlined the impact of cyber security incidents and the contribution of the human component and associated systemic failures. This section explores some of the broader concepts in detail.

3.1 Behaviour change

When it comes to tackling human vulnerabilities, a common approach has been to provide people with training and education. However, people still exhibit risky security behaviours in practice. A common misunderstanding is that if people complete training and know what to do, they will change their behaviour. However, knowing what to do, and how to do, it is not enough. HF experience shows that systemic failures are the cause of most incidents, and no amount of training or e-learning can force people to 'care'; "Everyone can make errors no matter how well trained and motivated they are" (Health and Safety Executive[25]). Organisations need to move beyond 'tick-box' training and towards focussing on behaviour change. To change behaviour in a sustainable way, we need to understand why behaviours are as they are and what needs to change for desired behaviour change. Why do people download sensitive information to personal files? Why do people fall for phishing attacks? Answering these questions requires understanding what is driving risky security behaviour. The COM-B model of behaviour (Michie et al., 2011[26]) was developed as a simple model of behaviour change.

3.1.1 Behaviour change theory: the COM-B model

The COM-B model argues that behaviour is part of an interacting system of a person's capability, opportunity, and motivation. Encouraging a person to change their behaviour requires changing **one or more** of the COM-B components.

CAPABILITY is a person's psychological and physical capacity to apply a behaviour. In cyber security, we often refer to this as knowledge (such as having an understanding of cyber risks). However, a lack of capability may be connected to a person's skills (such as creating a password, detecting phishing heuristics); memory and attention processes (such as remembering passwords); and lack of self-regulation (inability to follow-through goals or intentions).

MOTIVATION is anything that energises and directs behaviour. Although people like to think they make conscious rational decisions, it is often fast, automatic processes that drive decisions[27]. These fast, more impulsive decisions are subject to a mass of mental shortcuts and biases. Biases help to speed up the vast array of information we process daily, but they can also lead to undesirable behaviour (such as opening attachments we know we shouldn't or clicking on links instinctively). For example, we tend to listen to information that confirms our preconceptions - a shortcut referred to as confirmation bias. Similarly, contextual bias could explain the success of targeted ('spear' and 'whaling') phishing emails. The slower, more reflective part of decision-making covers our attitudes and beliefs towards cyber security and its importance. Risk perception, a part of reflective motivation, is generally not considered to be a driver of security behaviours[28].

[25] https://www.hse.gov.uk/humanfactors/topics/humanfail.htm
[26] Michie, S., Van Stralen, M. M., & West, R. (2011). The behaviour change wheel: a new method for characterising and designing behaviour change interventions. Implementation science, 6(1), 1-12.
[27] Kahneman, D. (2012). Thinking Fast and Slow, First Edition, Penguin, ISBN-10 0141033576
[28] Renaud, K., & Dupuis, M. (2019, September). Cyber security fear appeals: Unexpectedly complicated. In Proceedings of the New Security Paradigms Workshop (pp. 42-56).

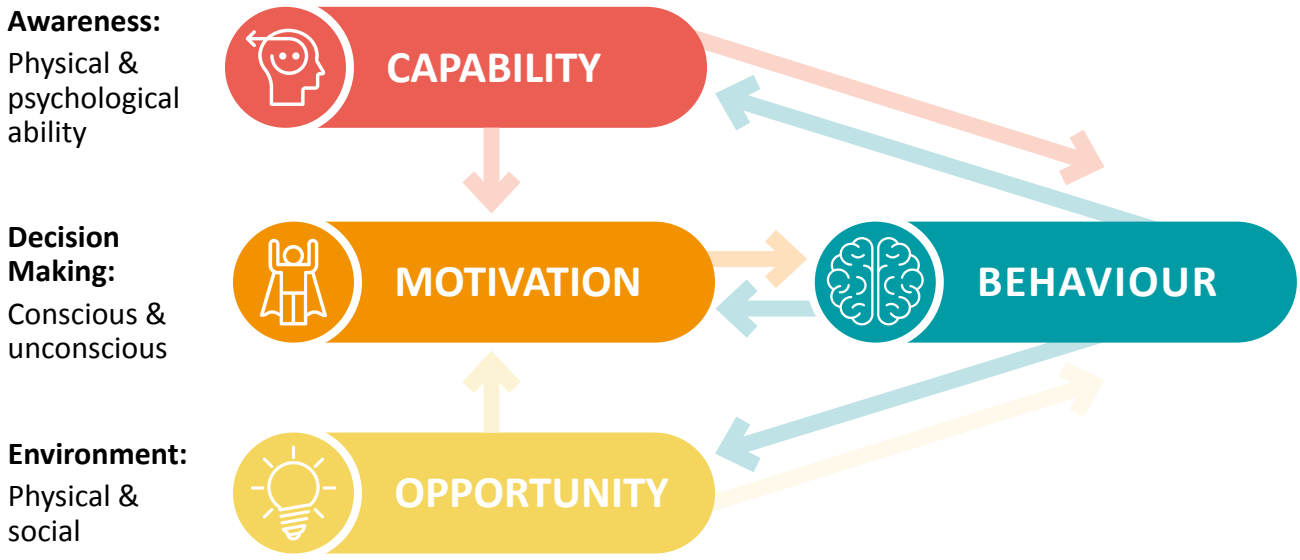


Figure 1 – COM-B model

OPPORTUNITY refers to external factors that makes being secure possible or impossible. The model describes physical and social opportunity. Physical opportunity consists of environmental factors like computer resources, security policies and building restrictions. Usable security may encourage people to engage with it. Social opportunity includes internal and external norms and cultural influences on behaviour.

3.1.2 Theory to practice

Having identified the behaviours that would increase the security of the organisation, such as using secure passwords or reporting suspicious emails/behaviour, ideally any opportunity barriers should be addressed first. Interventions focussed solely on capability and motivation can often be less effective when people lack opportunity. If possible, the most secure way of performing a task should also be the easiest way. An example of a physical opportunity barrier would be cyber security/information management policies that prevent information sharing with legitimate third parties, these may encourage people to look for unsecure workarounds. If it is impossible to remove opportunity barriers, or would require a significant amount of time, then there is still value to be gained from focussing purely on the capability and motivation aspects first. Training that includes relevant examples of incidents and vulnerabilities is particularly beneficial, and research has shown that building confidence and a sense of coping is more effective than risk communications that elicit fear and a feeling of susceptibility to threats[29].

The organisations' vision for its cyber security strategy should be encouraged and exemplified. This can be achieved if it is communicated by respected, likeable peers from diverse demographics. Incentives to change may be provided. For example, people could be encouraged to commit to a target such as the number of positive cyber security behaviours in a month. Recognising and publicising good performance allows people to feel good about themselves and creates a positive norm. Social opportunity is

[29]Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. Computers in Human Behavior, 87, 87-97.

facilitated when managers are good role models and exhibit good cyber security behaviours. Policies and procedures should be endorsed by senior managers. Risky behaviours need to be challenged so that they do not become norms; and good behaviours should be recognised and rewarded. These positive behaviours have been captured in the HACS Framework as quick wins and long terms solutions, to combat specified risky behaviours. Key recommendations:

- Training is not the *only* way to reduce risky security behaviours, instead consider *why* people may be doing these behaviours and address the root cause.
- Identify behaviours that increase the security of the organisation and consider what capability, opportunity and motivation people have for engaging in this behaviour.
- Add any potential "opportunity barriers" first, if possible, as these are often quick wins.

3.2 Cyber security maturity models

Maturity models establish a systematic basis of measurement. The classification mechanisms within a maturity model can help organisations assess their control and process management and, if necessary, to identify the actions necessary to improve the maturity of the organisation or process. A cyber security maturity assessment should address human, organisational and technical aspects. All phases of cyber security incident management, i.e., prevention, detection, response, forensics, and recovery[30] should be included. The 'level of maturity' includes the quality and the completeness of the implementation of each defence measure, as well as the acceptance of these measures by managers and employees. According to NIST (2008)[31], three types of Key Performance Indicators (KPI) for continuous cyber security monitoring may be defined: measures of implementation, effectiveness/efficiency, and impact.

Implementation measures assess the maturity of processes, procedures and security controls implemented in an organisation. After implementation, effectiveness/efficiency measures monitor these processes, procedures, and security controls, to determine whether they are operating as intended and meeting the desired outcome. Impact measures articulate the impact of cyber security on the organisation's mission. They may encompass security impact on the organisation's reputation, business, and economics goals.
All of these dimensions consider the integration of human, organisational and technical aspects. These considerations have been mapped to maturity levels and are presented in Table 1 opposite. A competent HF professional should be consulted to support the assessment of maturity level and implementation of recommendations.

[30]NIST (2014), Framework for Improving Critical Infrastructure Cybersecurity - Version 1.0, National Institute of Standards and Technology February 12, 2014
[31]NIST (2008), NIST Special Publication 800 – 55 Revision 1, Performance measurement Guide for Information Security

Table 1 - HF considerations mapped to NIST 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.
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

Table 1 - HF considerations mapped to NIST maturity levels (continued)

Maturity Level	Name	General Description
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.

Managers and employees need to be proactively involved in the design of an organisation's cyber security approach to facilitate compliance. This involvement encourages adoption of cyber security mitigation measures, reporting of cyber security incidents, and exchange of information and feedback. Proper training and communication can support the process and build an effective cyber security culture. However, these are not the only solutions.

3.2.1 Key recommendations

- Conduct a high-level assessment of cyber security maturity to identify areas to improve or consult with a competent HF professional to gain a detailed assessment of maturity level and implementation plan for recommendations.
- Once processes are in place, focus on measurement, continuous improvement and learning from experience.
- Include managers and employees in the design of the organisation's cyber security approach.

3.3 Organisational resilience

Organisational resilience can be defined as the ability of a system or organisation to monitor, anticipate, respond to, learn from, or recover readily from, a crisis or disruptive process[32]. To ensure an organisation has the resilience to withstand a cyber security threat or event and recover quickly, with minimal effect on its everyday business activities, it needs to have appropriate systems in place. Some organisations require exceptionally high resilience in the form of risk awareness and risk management, such as aviation, space, maritime, nuclear power, and military systems. In these cases, the costs of incidents, attacks and breakdowns are valued not only in economic terms but also in human lives. These organisations are often classified as high-reliability organisations (HROs)'. This means they aim to achieve error-free performance and safety in every procedure, every time — all while operating in complex, high-risk or hazardous environments, identifying and preventing potentially catastrophic

[32] https://erikhollnagel.com/onewebmedia/RAG%20Outline%20V2.pdf

incidents before they happen. For most organisations this level of resilience can be unnecessarily expensive to maintain, but the principles of self-improving, learning and adapting[33,34], can be applied at an appropriate level. The following paragraphs describe how organisations can monitor, anticipate, respond to, and learn from cyber security threats and incidents.

3.3.1 Monitor and anticipate

To respond to an incident, an organisation first needs to be made aware they are being attacked. Monitoring systems to facilitate quick detection of malware and potential HF-related insider threats, enhances cyber security resilience. A good security culture encourages users to immediately raise concerns via a robust, usable reporting system, without fear of retribution. Threats to cyber security can come from many different areas and as such, organisations need to ensure they have access to reliable information source(s) to monitor the latest trends in cyber security attacks, to ensure physical and system controls are constantly updated to manage the threat. Organisations need to keep abreast of the latest developments in cyber threats and put in place the necessary response measures to minimise potential business threats, for example, through threat briefs and malware trending. Using a variety of communication methods, they need to ensure their people are aware of the potential for cyber security attack. The intervention example in box 3 illustrates how cyber security awareness can be improved by using realistic attack examples and identifying employee cyber security champions. Many organisations also undertake proactive work using a person-based approach, with enhanced monitoring of people-of-interest.

BOX 3 **Intervention example, illustrating how to heighten security awareness**

The problem
A large company site had over 2,000 high risk employees with poor security awareness and behaviour.

The plan
In order to raise awareness of site-specific cyber security vulnerabilities, independent security personnel planned a social engineering attack on the site using manipulation of human vulnerabilities known as human hacking or social engineering. The attack simulation was intended to be incorporated in future training at the site, to make it personal and relevant. The simulated attack was designed to test unauthorised site entry and subsequent access to login details. Open Source Intelligence (OSINT) activities helped identify the site layout cameras, service doors, guards and reception areas, canteen, and floors. Employees and proposed targets including contact details, mobile phone numbers and email addresses, were identified. Employee social media accounts were identified and many pretexted communications were sent by the attackers, posing as employees, to gain further information.

The simulated attack
Three targets, identified from OSINT, were sent an email designed to look like a phishing email. The targets were then called three times to simulate a vishing campaign (fake phone (voice) calls designed to obtain information), as described opposite.

[33]Norlander, A. (2019). Societal Security: How digitalization enables resilient, agile and learning capabilities. In Larsson, A. & Teigland, R. (Eds.). Digital Transformation and Public Services (pp. 198-213). Open Access. London: Routledge. ISBN 978-0-3673-3343-0.
[34]Norlander, A. (2014). Analysing Tactical Cognitive Systems: Theories, Models and Methods. In Berggren, P., Nählinder, S., & Svensson, E. (Eds.). Assessing Command and Control Effectiveness – Dealing with a changing world. Ashgate. ISBN: 978-1-4724-3696-2.

Vishing call 1: One week before the simulated site attack
The team launched a pretext call impersonating the security team to ask if the employee had received an email, and if so, how it was handled. The employee was praised for responding appropriately. However, the team member expressed concern and said the email cyber team were reviewing it and might contact the target again over the coming week. The attacker asked about the target's availability for the week ahead and their location in the site.

Vishing call 2: One day before the simulated attack
The attackers conducted a pretext call pretending to be the cyber security team reconfirming the previous call. The employee was, again, praised for responding appropriately. This time, the caller said the cyber security team needed to adjust the employee's computer and would have engineers on site over the following few days. The attacker confirmed the employee' worksite, location, and desk and would contact the employee again when the engineer would arrive. They said the repair would only take one minute.

Vishing call 3: The day of simulated attack, on site
The attackers called the targeted employee to confirm the "engineer" would be on site, at their desk in fifteen minutes. They reiterated that the repair would only take one minute and said they were just finishing supporting another employee with the same issue. Attackers, dressed in fake uniforms and holding fake identification, assured the site security guards they were meeting specified important employees, (the names had been obtained from OSINT), and only needed access to the lower-threat, canteen area of the building. Once in the canteen, the attackers tailgated authorised personnel across the site. The attackers then telephoned the target and explained that the "engineer" had issues, and asked the targeted employee if they would arrange a room for the engineer. They also requested the targeted employee complete a form that captured login information. The employee was also asked to show the team around the systems. When the employee had done so, the attackers the employee to leave them in the room and enquired about the possibility of food and drink.

The outcome
Following the simulated attack, the target was fully debriefed and supported asked permission to use the story in proposed training for the site. They were also asked if they wanted to become a site security champion. Over 2,000 people were taken through face-to-face training in the first week. The training focused on how to stay protected in work and in their personal lives. The training covered both physical and cyber security topics such as: what is social engineering, insider threat, the risks, the criminal landscape and, why we fall for social engineering (the psychology). The session also included the role of security champions. Following the training, over eighty people volunteered to become security champions. A site champion team then worked together with the security teams to make over thirty-five security improvements to the site. Following the training and ongoing improvements, the site security risk assessment classification changed from high, to low risk.

3.3.2 Respond

3.3.2.1 Immediate response

Once aware of an issue, specialist cyber security knowledge is needed to make the system safe, carry out initial actions (immediate containment, and preventative actions such as briefing staff). The board need to know what to do, and who to contact, in response to a cyber security incident (see section 3.4 for more detail). Availability of expert resources is necessary to facilitate a fast response to a cyber security threat. In-house expertise in large organisations, or immediate access to external resource for smaller businesses, should be planned. Many organisations adopt a hybrid model, with in-house expertise and a call-off contract for additional specialist resource when needed.

3.3.2.2 Post incident response (learn)

Once the system is fully restored and actions have been undertaken to ensure the system is safe, a review of an incident by a problem management team provides an excellent opportunity to take stock of what worked, what didn't, and what can be done better in a future similar incident. The purpose of the review is to encourage open and honest interviews with the subject matter experts and stakeholders who were involved in the incident. It is extremely important to create an environment where people can reflect and raise ideas. These conversations support root cause analysis.
Root cause analysis is the structured means of understanding what happened and why, by considering immediate, underlying, and root causes of an event. It is usually undertaken following an event or incident to identify causes and find corrective and preventative actions to address any vulnerabilities. It is important that the root cause analysis is conducted by a multi-disciplinary team. The investigation should consider multiple organisational and situational causes and avoid starting with a single cause in mind. There are a number of models that can be used to inform root cause analysis such as Serrat's 2009 '5 whys' technique[35]. They can be used to identify potential HF-related vulnerabilities that contributed to an incident. The behaviours, causes and recommendations in the HF cyber security framework (section 3.0) can be consulted retrospectively, to determine the human-related root causes of an incident. The investigation team should be multi-disciplinary, to ensure incidents are addressed from different perspectives, and should generate Specific, Measurable, Achievable, Specific, Relevant, Time-bound (SMART)[36] actions to reduce the risk of recurrence of a similar incident. Actions might include updating policies, procedures and training material; system development; and a resource review to ensure there is sufficient access to expert knowledge. A critical part of the post incident review is the communication plan. Communication should be clear, targeted, current and fluid across the business. The communications should contain information about the incident and how to prevent it and any resultant changes to policies and procedures. The process should also ensure outcomes and lessons learned are shared and networked across the business and industry to help anticipate and respond to future incidents.

3.3.3 Key recommendations

- Conduct monitoring and assess threat intelligence to know when attacks are happening and to identify the latest trends in cyber security attacks.
- Foster a just culture to encourage employees to immediately raise concerns without fear of retribution and have a usable reporting system.
- Learn from incidents by applying root cause analysis and assigning SMART actions.
- Communicate the results of incident investigations and any associated changes to internal personnel (potentially with other organisations).

[35]The Five Whys Technique | Asian Development Bank (adb.org)
[36]Based on Doran, G. T. (1981). There's a S.M.A.R.T. way to write management's goals and objectives. Management Review. 70 (11): 35–36

3.4 Board-level decision-making

The board[37], or equivalent body, is tasked with directing the organisation and ensuring its prosperity within its regulatory jurisdiction. When it comes to cyber security, however, many boards feel ill-equipped to deal with cyber security challenges. Few directors have confidence in their organisation's cyber security with only 10% of organisations having a dedicated cyber security committee overseen by a board member; this is expected to rise to 40% by 2025[38]. Board members feel that they do not have enough knowledge of cyber security to fully understand the potential risks and determine preventative measures[39]. Several barriers have been identified including time constraints (for example, only meeting quarterly and not sufficiently allocating time to discuss cyber issues; no dedicated budget for their cyber security strategy, differing reporting structures and lack of adequate reporting. [40]There are a wide range of cyber security frameworks and standards (such as NIST, COBIT and ISO27000) available to organisations[41]. However no best practice framework exists for board-level engagement. One example of a governance model is the 'Three Lines of Defence'[42]. 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. However, the lack of best practice consensus in adopting a framework or model can result in highly diverse executive approaches to cyber security risk management (in terms of reporting intake, reporting mechanisms, and ownership of governance functions).

Chief information security officers (CISO) may report directly to the chief executive officer (CEO) or to other roles, such as chief security officer (CSO) or chief finance officer (CFO). This reporting separation may mean cyber security issues may not always be reported as intended[43]. Research also highlights a lack of consistency in reporting content between the requirements of board executives for clear, relevant content and the deliverables reported to the board. Board executives should be informed on cyber security in accessible, non-technical language to help them understand the risks and implications of their decisions[44]. The discipline of HF enables efficient organisational design and decision-making and can support this process for cyber security.

3.4.1 Key recommendations

- Cyber security risk management should be shown to align with an organisation's overall business strategy to fully engage the board.
- Use toolkits, like the National Cyber Security Centre (NCSC) board toolkit[45] that provide practical guidance on engaging the board. The recommended risk assessments should include HF considerations.
- Streamline reporting processes, for example, enabling direct communication between the CISO and the CEO.

[37]This paper refers to the "board" in terms of the directors of an organisation, however the content is equally applicable to any senior-leadership decision makers of organisations that may or may not have a board of directors.
[38]Gartner (2021). Gartner Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025 . Retrieved from https://www.gartner.com/en/newsroom/press-releases/2021-01-28-gartner-predicts-40--of-boards-will-have-a-dedicated-
[39]Ernst & Young. (2018). EY Global Information Security Survey 2018–19. Retrieved from: https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf
[40]Dynamics and Osterman Research (2016). Reporting to the Board. Retrieved from: https://baydynamics.com
[41]Moore, T., Dynes, S., & Chang, F. R. (2016). Identifying how firms manage cybersecurity investment. University of California, Berkeley.
[42]Deliotte. 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
[43]Tech, G., & Lee, W. (2015). Governance of Cybersecurity: 2015 Report How Boards & Senior Executives Are Managing Cyber Risks. Retrieved from: https://globalcyberrisk.com/wp-content/uploads/2012/08/GTISC-GOVERNANCE-RPT-2015-v15.pdf
[44] https://www.gov.uk/government/news/uk-boards-of-biggest-firms-must-do-more-to-be-cyber-aware
[45]https://www.ncsc.gov.uk/collection/board-toolkit

3.5 Presentation of cyber security information

In managing cyber security, like managing patient safety in healthcare, encouraging positive behaviours (see section 3.1) is vital but should be considered the last control measure. What can be changed more quickly, and has a significant effect on cyber security risk, is the design of the tools and systems that workers use. The application of HF engineering principles to design can prevent the mistakes that lead to the realisation of threats. The previous section 3.4) identified the need for enhanced presentation of information to the board. Most of the design inadequacies in current dashboards are in the domain of cognitive ergonomics; the HF scientific discipline that draws upon research of how we perceive and process information and make decisions about it. Effective decision-support design is more complicated than might be obvious, even with relatively simple goals. Design that can give chief information officers (CIO) and CEOs confidence that cyber security risks will be appropriately managed relies on three critical success factors:

1. Clear understanding of the specific decisions that users are expected to make based upon the cyber risk information presented – identifying information needs.
2. Understanding how people perceive information and factors which bias or prejudice perception and decision-making; and
3. Usability testing of human decision-making performance; not merely user preference.

These critical success factors are part of adopting a user-centred design approach, as outlined in ISO 9241-210 Human Centred Design for Interactive Systems[46], and are discussed further in the following sections.

3.5.1 Identifying information needs

The first success factor refers to clear understanding of the specific decisions that users are expected to make based upon the cyber risk information presented. This understanding should be jointly held by users, their managers, and the system designers. Cyber security personnel need to know:

- *What am I seeing?*
- *Is there a pattern?*
- *Is something abnormal?*
- *What does it mean?*
- *What should I be doing?*

CIOs and CEOs want assurance related to their common concerns:

- *What are my people seeing in relation to cyber threats?*
- *What could they be missing / not seeing?*
- *How effectively are they reacting to threats?*
- *How efficiently are they reacting to threats?*

Design for decision orientation can be achieved by asking questions such as “What’s the problem?”, “How bad is it?”, “How bad could it get?”, and “What can be done?”. Consulting representatives of the intended user population is necessary to identify whether the required information is presented and likely to be understood.

3.5.2 Understanding what influences perception and decision-making bias

The second critical design success factor refers to the need to understand what influences perception and decision-making. Use of design elements typically associated with danger, warnings, or risk (e.g., use of red, flashing, bold, capitals, exclamation marks, etc.) without consideration of HF, may prevent the intended effect. Consistent presentation of information, where items with similar intent are presented similarly is recommended to reduce the likelihood of error[47].

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

Human decision-making is also subject to a many critical biases which could affect presentation of cyber security information. They include the tendency to think things are more important or relevant if they are more:

- Recently presented (assumed to be more up to date)[48]
- Presented first, a concept termed 'anchoring'
- Salient (or more prominent—loud, bold, red, etc.—than other things around it)
- Available (e.g., more quickly found in searching)
- Common (volume of similar data tends to outweigh judgement of relative reliability)
- Apparently representative (relying upon subjective assessment of probability)[49].

Confirmation bias is defined as the tendency to "seek (and therefore find) information that confirms the chosen hypothesis"[50]. It is strong because changing hypothesis requires greater cognitive effort than maintaining the same hypothesis and it is harder to deal with negative than positive information. All these biases conspire against detecting and acting upon the most significant cyber security threats because the voluminous, repetitive, most available information may not be associated with what is the most dangerous threat. For example, a prominent denial-of-service cyber security attack may demand more attention because it generates more information/messages. However, it may be less dangerous than quietly injected malware that obtains sensitive information.

How well we make decisions also depends heavily on how they are framed. Beyond normal operational jargon, the IS domain is burdened with overly dramatic language. Words like "kill", "terminal", "fatal", "catastrophic", and "firewall" appear frequently in error or status messages, desensitising users to what might be critical. A "brute force attack" for example, may sound more aggressive, and generate a higher, more salient volume of network activity and corresponding information in the dashboard, but, often has lower overall damage potential than an 'infection' of malware. In summary, presentation of cyber security information should be cognisant of human decision-making biases.

3.5.3 Usability testing

There is a need to consider not only the user experience of the design, but also their associated performance. Much like safety critical systems, cyber security usability testing should measure the effectiveness and efficiency with which users can accomplish their cyber security goals. The standard ISO 9241-11[51] defines effectiveness and efficiency as follows:

- Effectiveness is measured as the accuracy, completeness, and lack of negative consequences with which users achieved specified goals. Measures include number of tasks completed correctly and number of errors.

- Efficiency is the measure of effectiveness divided by the resources used in achieving the level of effectiveness. Example measures include time taken to perform a task, cost, and fatigue.

3.5.4 Key recommendations

- It is important to consider the presentation of information for effective decision-support, especially when considering off-the-shelf purchases of cyber security dashboards. HF professionals can support this activity.
- Consideration should be given for the specific decisions that users are expected to make based upon the information presented as well as how people perceive this information, including decision-making biases.
- Usability testing should be undertaken to measure the effectiveness and efficiency with which users can accomplish their goals.

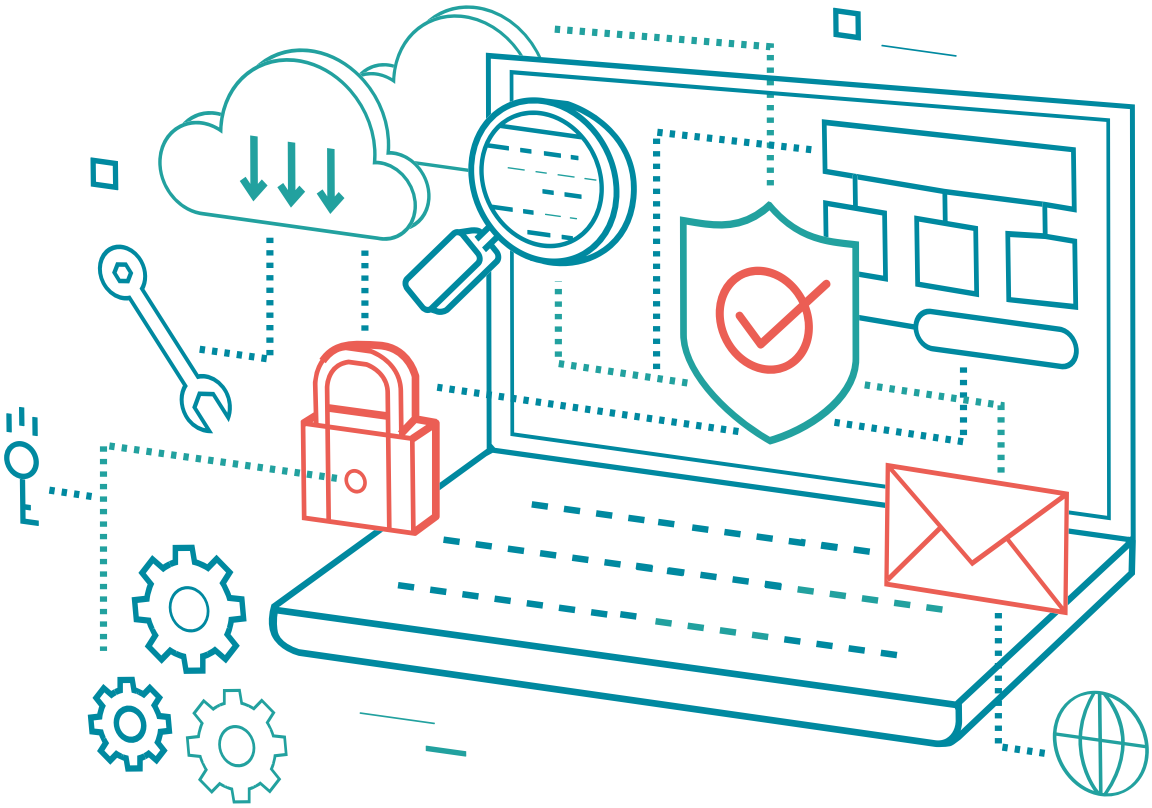
[47]BS EN ISO9241-112 BSI, Ergonomics of Human-System Interaction (2017) Part 112; Presentation of Information
[48]Ebbinghaus, H., (1913), On memory: a contribution to experimental psychology, New York: Teachers College
[49]Wickens, C.D, 1992, Engineering Psychology and Human Performance, second edition, Harper Collins (pubs), ISBN 0-673-46161-0
[50]Wickens, C.D, 1992, Engineering Psychology and Human Performance, second edition, Harper Collins (pubs), ISBN 0-673-46161-0
[51]ISO 9241-11: Usability: Definitions and Concepts and 5 ISO/IEC 25022: Measurement of Quality in Use.

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 factor in such incidents but is rarely the root cause. Instead, the root cause is often a systemic, organisational failure that, unless addressed, will continue to influence organisational cyber security performance. HF professionals can assist with the assessment of organisational causes and recommend appropriate solutions.

Section 3.0explored some broad HF considerations to support cyber security decision makers. Considerations included behaviour change; cyber security maturity levels; organisational resilience; board-level decision-making; and presentation of cyber security information. Key recommendations have been summarised at the end of each subsection.

A HF cyber security framework has also been developed (ref) alongside this paper that presents lower level, specified, undesirable behaviours and associated solutions. It was designed to be used by HF professionals and 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) have also been included; however, the recommended solutions largely pertain to changes at a system or organisational level which can reduce risk of human-related cyber security incidents.



5.0 Authors, contributors and reviewers

5.1 Authors and contributors

- Nicola Turner, Senior Human Factors Scientist, Trimetis, UK
- Amanda Widdowson, CIEHF Past President, Head of Human Factors Capability, Thales UK
- Dr John Blythe, Director of Cyber Workforce Psychology, Immersive Labs, UK
- Khaled Simmons, Director, Ergoworks, UK
- Clare Pollard, AWE, UK
- Mike Fortune, Security Behaviours – Industry Subject Matter Expert Social Engineering -Insider Threat -Human Behaviour - BT plc, UK
- Dr Arne Norlander PhD, CEO & Chief Scientific Officer, NORSECON, Sweden
- 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

- 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
- Simon Pavitt, Head of Cyber Awareness, Behaviours & Culture, Ministry of Defence, UK

Chartered Institute
of Ergonomics
& Human Factors

www.ergonomics.org.uk

ciehf@ergonomics.org.uk

Designed for CIEHF by Connect Communications – connectmedia.cc