Human Factors in Rail Cyber Security

Amanda WIDDOWSON

Thales Cyber and Consulting, UK

Abstract. The majority of cyber security incidents cite the human element as a contributory factor. Information Security systems that rely on operators remembering lengthy, complicated passwords and following procedures that do not consider job requirements or psychological motivations, are not adequate protection. Computerised signalling and electrical control systems increase vulnerability to cyber attack. Further technological advances could exacerbate this vulnerability. The Cyber Human Error Assessment Tool (CHEAT) is a structured approach capturing human-related risks in cyber security.

Keywords: Cyber security, risk assessment

1. Introduction

Cyber security is a growing issue. The National Security Strategy (HM Government 2015) presented cyber security as one the most significant threats to the UK. The National Cyber Security Centre (NCSC) was launched in February 2017 in response to this threat. Advances in technology bring considerable benefits to the way we work and live, but they also increase our vulnerability to cyber attack. Rail cyber security guidance observes: "Railway systems are becoming vulnerable to cyber attack due to the move away from bespoke stand-alone systems to open platform, standardised equipment built using COTS components and increasing use of networked control and automation systems that can be accessed remotely via public and private networks" (Department for Transport, 2016).

So how do we defend rail systems from cyber attack? Many approaches consider technical protection mechanisms, yet evidence suggests that the majority of cyber security incidents are caused by the human element. IBM reported that the majority of cyber attacks in 2014 were caused by insiders and "over 95% of… (insider) breaches are caused by human error" (IBM 2015). They later reported that "60% of all (cyber) attackers are insiders" (IBM 2016). This suggests that the discipline of human factors has a large part to play in understanding and addressing cyber security incidents. Recent research supports the view that a sociotechnical approach is needed, rather than a purely technological (or social) one (Coles-Kemp, 2017). However, further observations indicate that "Despite the intrinsically psychological nature of cyber security attacks, research into the role of psychology in cyber security is still limited" (McAlaney et al., 2016).

Recent research that considers this 'Insider Threat' is often focused on the malicious insider and how to identify malicious behaviours (Nurse et al., 2014; Rashid et al., 2016; McAlaney et al., 2016; Meeks, 2017). Indeed, current rail cyber security guidance (Department for Transport, 2016) states the "main focus of …guidance is on deliberate attack". The motivations behind malicious insider attack are an important consideration in tackling cyber crime. However, figures based on 2016 cyber attacks indicated more insider attacks were

completed by inadvertent actors than malicious insiders (IBM 2017). 'Inadvertent actors' refers to people who unintentionally cause or contribute to a cyber attack. For example, by unintentionally activating malware in spam email, or losing confidential data. Human error analysis is already conducted to support rail safety cases, so it is possible to adapt this knowledge to cyber security scenarios. The rail guidance (Department for Transport, 2016) acknowledges the need to consider "non-deliberate attack through unintended infection with malicious software…non-deliberate security breach through negligence or lack of knowledge."

The Cyber Human Error Assessment Tool (CHEAT) was developed to capture and mitigate human-related risks (unintentional and malicious) in cyber security, and human-related causes/contributory factors in post incident investigations (Widdowson and Goodliff, 2015). The tool was developed by drawing on applied experience of Human Reliability Analysis (HRA); existing principles of cognitive, organisational and social psychology; and analysis of human error as part of rail safety investigations. Data is collected using targeted, structured interviews and a questionnaire. CHEAT incorporates automated reporting technology to ensure fast collection of human-related risks. Reports include numerical risk scoring and prioritised mitigating solutions.

Since its first publication in 2015, the approach has been successfully applied in the defence sector, where the human element is considered to be a critical part of Cyber Vulnerability Investigations (CVI). It also has potential application in rail. The paper will describe the approach and its relevance to the rail industry, with reference to redacted case-studies from the defence industry.

2. CHEAT overview

An overview of CHEAT is presented here. For more detail, see previous publications (e.g. Widdowson and Goodliff, 2015; Widdowson 2016).

2.1 Model development

CHEAT was developed by reviewing cyber security incidents to identify the human-related root causes. This was facilitated by applied experience of human factors in formal rail safety investigations. Incidents included the 'Sandworm' phishing email attack, which affected NATO, academic institutions, communications and energy organisations; and generic social media and dating website vulnerabilities. The review was limited by the apparent reluctance of some organisations to admit that they had been attacked. This may be because of fear of reputational damage.

Over 40 platform agnostic human vulnerabilities threat indicators were identified from the incident review and applied HRA knowledge. At least one mitigating recommendation was identified for each indicator. The indicators were arranged into four categories: People, Organisation, Environment and Technology (Figure 1). By their nature, some indicators span multiple categories. For example, a training provision indicator pertains to the organisation category, but individual awareness of cyber security (derived from training) is a people factor.

Example vulnerabilities from each category are described in the following paragraphs.

Figure 1 - CHEAT categories

2.2 Physical environment vulnerabilities

Analysed incidents included attacks achieved by access to Barclays and Santander computers in 2013. Cybercriminals entered high street branches of the banks and pretended to be from the company Information Technology (IT) department. In this way, they gained access to the computer system and stole customer banking information. This illustrates that a weakness of technical control systems is the human operator(s). Why did the banking staff trust the attackers? Perhaps they were used to visits by IT staff they did not know. Politeness and social compliance may have prevented them from requesting identification. Diffusion of responsibility (Darley and Latané, 1968) may explain why no individual member of staff questioned the presence of the attacker. The criminals may have seemed very likable and evidence suggests we tend to trust people we like (Eagly and Chaiken, 1984). Social psychology clearly has a part to play to help us understand this behaviour. This analysis led to the development of human vulnerability threat indicators pertaining to the physical environment. If people are used to seeing strangers in their working environment, they may be more likely to trust an attacker who has gained unauthorised entry.

Another physical environment consideration is 'tailgating'. This is where employees allow attackers entry to secure buildings by holding doors open. Politeness and social compliance may prevent people from closing the door on others or asking for credentials, in the same way that the banking staff allowed access in the incident described earlier. This human vulnerability can be mitigated by automation such as turnstiles and/or an intermittent security presence. A named security individual, with responsibility for building access, mitigates the risk of diffusion of responsibility. Signage may also help. This allows people to point to the signage and blame 'rules', to explain their need to see authorisation or refuse tailgating.

2.3 Organisational vulnerabilities

Organisational considerations include policy and procedures; cyber security awareness training; personality screening; and general organisational culture. An organisation's cyber security policy and procedures should be designed around the work of its employees. Security behaviour guidance indicates "if employees believe there are too many hurdles or barriers to applying the (secure) behaviours….they will be less likely to do so" (CPNI 2017). Recent UCL research found employees "too often" had to choose between "complying with security and getting their work done" (Sasse, 2016). If procedures fail to take into account employees' need to complete their work, the employees may invent unsafe 'workarounds' to circumvent the procedures (Widdowson and Goodliff, 2015; Sasse, 2016). CHEAT includes a

vulnerability indicator and recommendations regarding policy and procedure design, access and endorsement by senior management. Organisational change literature pertaining to cyber security culture (CPNI, 2016) supports the view that management endorsement and leading by example increase the likelihood of employee compliance. Supplier cyber security policy is also addressed.

Cyber security awareness and training is cited as a vulnerability in rail guidance (Department for Transport, 2016). CHEAT data collection assesses the quality of training and competence management, and recommendations describe the desired content of the training. Training that contains examples that are relevant to the target audience is more likely to be successful. Beyer et al., 2015, support this view, stating training "must be tailored to specific groups of employees, and deliver a core set of skills that are relevant to their productive tasks."

A review of personality tools identified traits that may be associated with cyber security vulnerabilities (Widdowson and Goodliff, 2015; Widdowson, 2016). The vulnerabilities pertain to unintentional; intentional, non-malicious; and malicious Insider Threat. These traits are already captured by many organisations as part of recruitment and development. Therefore, existing data can be analysed to identify potentially vulnerable individuals.

2.4 People vulnerabilities

The People category comprises vulnerability indicators such as password design and cognitive biases. Lengthy, complicated passwords challenge human memory capacity. Users may be tempted to write passwords down, store them in their mobile phone, and/or use the same, easy-to-guess password for multiple work and personal applications. Consequences of this were illustrated by the recent attack on the UK Parliament in London, which was reportedly caused by "weak passwords" (BBC, 2017). Lipford reported that changing passwords every few months encouraged people to reuse the same ones (Sasse et al., 2016). The user may recognise password misuse as a deliberate violation of cyber security policy, but the consequences of compliance may adversely affect their ability to their job.

Cognitive biases, such as contextual bias, may affect the likelihood of success of a spear-phishing email attack. In practice, we decided to reserve many of the cognitive biases in the CHEAT tool for post-incident investigations or assessments of small groups. This is because we all may be equally susceptible to various cognitive biases, and assessing the risk on an organisational level could generate inaccurate results.

2.5 Vulnerabilities in the use of technology

Technology considerations in CHEAT include the use of social media and trust in technology. We can assess whether people talk about work on social media (therefore potentially revealing competitively sensitive information or making themselves targets for attack). Malware is also shared via social media. Trust in this case refers to over-reliance on cyber security technology such as anti-virus software. It also considers the user's trust in the information they receive from technology.

3. CHEAT Method

The CHEAT application process is illustrated in Figure 2. An initial planning stage is designed to establish the boundaries of the assessment in terms of departments, sites, staff numbers and timescales. Data collection interviewees and questionnaire recipients are also identified and the operational scenario is defined at this stage. The high level impact of a cyber attack and data loss, for the organisation in question, may also be determined during the planning stage.

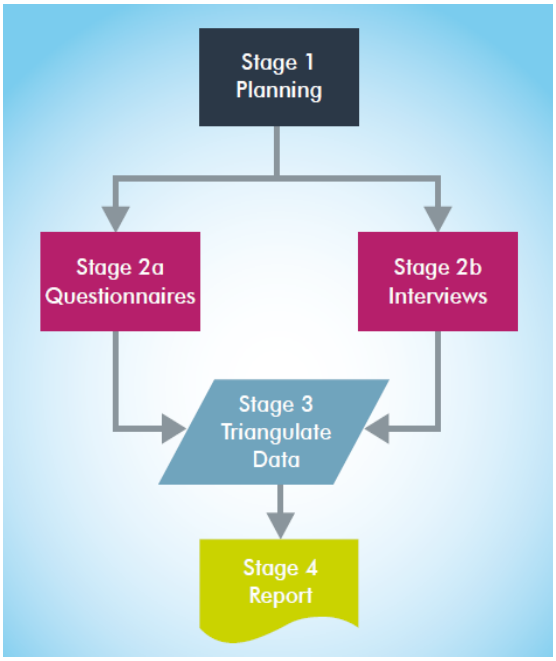

Figure 2 - CHEAT process

CHEAT utilises two forms of data collection to ensure a robust approach. Questionnaires are designed to capture data from a large, remote audience. Structured interviews allow more detailed questioning and discussion from individuals with specialist knowledge. Key interviewees are representatives from: Information Security (IS); buildings security; Human Resources, recruitment and cyber security training; and technical role representatives. The interviews and questionnaires contain generic questions but can be tailored to a given operational area or platform.

The likelihood, impact and risk of each indicator, in the organisation under assessment, are derived from data collected from the questionnaire and structured interviews. The data is automatically combined and automated reports are generated.

CHEAT was initially produced and applied in spreadsheet format in 2015. In 2017, a software application version was produced to further enhance the speed and efficiency of data collection and automated reporting. As shown in the menu (Figure 3) automated reports include graphical representations of the average risk score per category (spider diagram); the number of high, medium and low risks (pie-chart); and a recommendations bar-chart. The bar-chart presents the number of high, medium and low recommendations. The ease of implementation of the recommendations in terms of time and cost (Easy, Average, or Difficult) is also incorporated in the bar-chart. An example automated pie-chart and bar-chart are shown in Figure 4.

Figure 3 - Automated results report menu

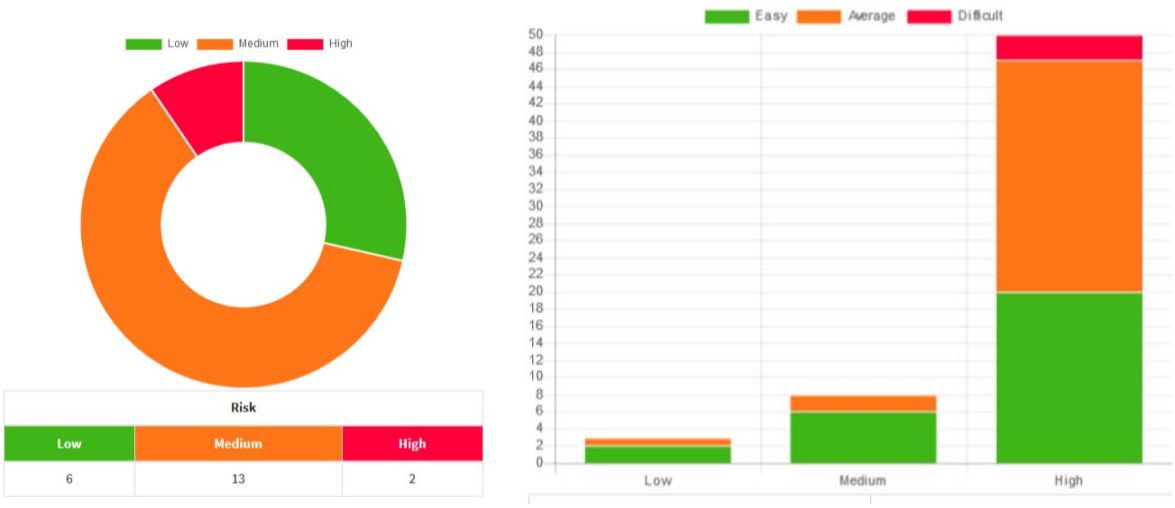

Figure 4 - Automated results report examples

The graphical reports are accompanied by a textual summary report of automated recommendations. These recommendations are prioritised by risk and ease of implementation (time and cost) and are associated with the relevant human vulnerability indicators. The form comparison report, shown in the results menu in Figure 3, allows the analyst to compare the results from each interview and the questionnaire results. For example, it may be interesting to compare the view of cyber security training provision from the training provider/manager and the questionnaire respondents. Any findings from this review are discussed in the final report.

An overall risk score is also provided. This represents the actual risk score as a percentage of the maximum possible risk score. This score can be identified before and after the implementation of mitigating recommendations, to demonstrate a reduction in risk. A further benefit of this high-level statistic is a department can be compared with other departments or programmes within an organisation, to determine the highest risk department(s). Repeated application of the tool will facilitate the generation of an industry norm score. This can then be used as an indicator of what good looks like.

The automated reports are reviewed by a trained human factors analyst, before a final report, comprising quantitative and qualitative analysis, is produced. Applied examples of the method are described in Section 4. Additional assessments are ongoing.

4. Case studies

Two recently applied CHEAT assessments are presented in this section. Information has been restricted for security and confidentiality reasons.

4.1 Airborne surveillance and control project team (2017)

CHEAT was applied to a team supporting the provision of airborne surveillance and control capability. Data was collected from eight semi-structured interviews with key roles. In addition, a questionnaire was distributed to 83 members of the project team and achieved a 45% response rate. 60 prioritised recommendations were automatically generated. Bespoke recommendations were also presented in risk statement format, with associated mitigations.

Example risks and mitigations pertained to password management, environmental working conditions, incident investigation, personnel screening, training and policy. An overall numerical risk score allowed comparison with future assessments on other organisations and repeated testing of the same organisation after implementation of priority recommendations, to demonstrate a reduction in risk. The report was well-received and the programme director stated "The CHEAT assessment identified vulnerabilities and practical recommendations to strengthen our defences against cyber attack."

4.2 Secure networks department (2016)

CHEAT was used to assess the impact of an attempted cyber attack on the secure networks department of a major defence contractor. Questionnaires were distributed to 15 members of the department. Respondents included Network Operation Centre (NOC) personnel, Network Architects, a Server Specialist and an Information Assurance consultant. A 100% response rate was achieved. Interviews were conducted with representatives from this group and the key roles described in section 3.

The CHEAT team made a number of suggestions, including simple, cost-efficient adjustments to the company's cyber security policy to enhance awareness and accessibility. The need for human factors input to future incident investigations was also recommended. The prioritised recommendations facilitated allocation of resources for maximum impact. The department head reported that the "CHEAT approach identified issues we hadn't thought of, as well as useful recommendations to reduce our risk."

5. Discussion and Conclusion

Rail cyber security guidance (Department for Transport, 2016) demonstrates awareness of the "potential for cyber attacks to cause damage and loss to rail networks." Advances in technology can enhance the efficiency of rail operations and maintenance, but they also increase vulnerability to cyber attack. Example target areas could include computerised signalling and electrical control systems; asset management systems; in-cab signalling systems; line-side equipment and, potentially in the future, voice-controlled autonomous agents in cabs and control rooms. If these systems were compromised, an attacker could possibly take control of trains, causing them to stop, effecting loss of service and tunnel evacuations; or worse, collide. Traction power could be turned on or off with potentially catastrophic safety, financial and reputational consequences. Information about future programmes, costs and progress is also at risk from 'hacktivism'.

The attack on Ukraine in 2015 demonstrated the real likelihood and consequences of a control room employee opening a malicious email. In this case, the malware activated by the email allowed attackers to access login credentials and shut-down electrical substations. The result was a loss of power to approximately quarter of a million customers in Kiev. Rail electrical and signalling control rooms are also at risk.

Human factors can play a significant role in the risk assessment and mitigation of cyber security attacks. Lessons learnt from the considerable application of HRA and incident investigation techniques in the rail sector, can be applied to address the cyber security problem. Just as HRA tools like the Human Error Assessment and Reduction Tool (HEART, Williams, 1986) and the Technique for Human Error Rate Prediction (THERP, described by Kirwan, 1994) have been consistently used to support safety cases in multiple industries, (e.g. rail, nuclear, oil and gas), we can apply our understanding of human vulnerabilities to cyber security scenarios in multiple sectors, including rail.

Useful cyber security guidance such as the '10 steps' (CESG, 2015) advocates the need for user training and policy design, including consideration of remote working, removable media and incident management, as well as technical solutions. Rail guidance (Department for Transport, 2016) proposes training to address the human risks. However, training and organisational cultural assessment approaches (e.g. CPNI, 2016) are not the whole solution; "We all make errors irrespective of how much training and experience we possess or how we are motivated to do it right." (HSE, 2009).

Other approaches have focused on malicious insider threat. However, we also need to consider unintentional actions, including human error, that can cause or contribute to a cyber attack, especially as the majority of incidents have been caused by the inadvertent actor (IBM, 2017). Tools such as CDCAT® (APM Group et al., 2017) include consideration of 'human interaction' in terms of security vetting and social media compliance. However, guidance regarding the detailed human factors aspects of cyber security, and how to mitigate them, is still evolving.

The CHEAT approach was designed to capture and mitigate human vulnerabilities in cyber security. The tool allows the analyst to identify priority areas of concern to facilitate targeted resource investment to address vulnerabilities. Applied experience has demonstrated that mitigating solutions can be inexpensive 'quick wins'. CHEAT has been repeatedly demonstrated in the defence industry and can be applied to existing and future rail operations, to drive down the risk of cyber attack.

References

APM Group, Ploughshare Innovations, Dstl, (2017). Cyber Defence Capability Assessment Tool (CDCAT®). Improving cyber security preparedness through risk and vulnerability analysis. Retrieved August 8, 2017, from https://apmg-cyber.com/products/cdcat.

BBC. (2017). Parliament cyber-attack 'hit up to 90 users'. Retrieved August 9, 2017, from http://www.bbc.co.uk/news/uk-40398696.

Beyer, M., Ahmed S., Doerlemann, K., Arnell, S. Parkin, S., Sasse, MA, Passingham, N. (2015). Awareness is only the first step: A framework for progressive engagement of staff in cyber security. (Business White Paper, Hewlett Packard Enterprise).

CESG (2015). Guidance. 10 Steps: Summary. Retrieved August 8, 2017, from https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary.

Coles-Kemp, L. and Hansen, R.R. (2017). Walking the line: The everyday security ties that bind. In Proceedings of Human Aspects of Information Security, Privacy and Trust, 5th International Conference, HAS 2017, Held as part of HCI International 2017, Vancouver, BC, Canada. Springer ISBN (electronic) 978-3-319-58460-7.

CPNI (2016). SeCuRE3 CPNI's cyber security tool. A Guide for national infrastructure organisations. Retrieved August 8, 2017, from

https://www.cpni.gov.uk/system/files/documents/d7/06/SeCuRE-tool-guide-for-national-infrastructure-organisations.pdf.

CPNI (2017). Embedding behaviour using the 5Es. A framework for improving security behaviour within organisations. Retrieve August 8, 2017, from https://www.cpni.gov.uk/system/files/documents/98/dc/Embedding-Security-Behaviours-Using-5Es.pdf.

Darley, J.M. and Latané, B. (1986). Bystander intervention in emergencies: Diffusion of responsibility. Journal of Personality and Social Psychology, 8, pp. 377-383.

Department for Transport, (2016). Rail Cyber Security Guidance to Industry. OGL.

Eagly, A.H., Chaiken, S., (1984). Cognitive theories of persuasion. In Berkowitz, L. (Ed.), Advances in Experimental Social Psychology. New York Academic Press.

Health and Safety Executive, (2009). Reducing error and influencing behaviour. HSG48. HSE Books. ISBN 978 0 7176 2452 2.

HM Government (2015). National Security Strategy and Strategic Defence and Security Review 2015. A Secure and Prosperous United Kingdom. Cm961. ISBN 9781474125963. OGL.

IBM Security. (2015). IBM X-Force Threat Intelligence Index 2015. Analysis of attack and incident data from IBM's worldwide security services operations. Research report. IBM Corporation.

IBM Security. (2016). IBM X-Force Threat Intelligence Index 2016. Reviewing a year of data breaches, major attacks and new vulnerabilities. Analysis of attack and incident data from IBM's worldwide security services operations. IBM Corporation.

IBM Security. (2017). IBM X-Force Threat Intelligence Index 2017. The year of the mega-breach. IBM Corporation. Retrieved June 1, 2017, from https://www.ibm.com/security/data-breach/threat-intelligence-index.html.

Kirwan, B. (1994). Technique for human error rate prediction (THERP). In Swain, A.D., Guttman, H.E. (Eds.), A practical guide to human reliability assessment (Chap. 5, pp.244-255). Taylor & Francis.

McAlaney, J., Thackray, H., and Taylor, J. (2016). The social psychology of cyber security. In The Psychologist, September 2016, Vol.29 (pp. 686-689). The British Psychological Society.

Meeks, R. (2017). The cuckoo's egg: identifying and revealing insider threat. In The Ergonomist July-August 2017 (pp. 22-23). The Chartered Institute of Ergonomics and Human Factors.

Nurse J.R.C., Legg, P.A., Buckley, O., Agrafiotis, I., Wright, G., Whitty, M., Upton, D., Goldsmith, M., Creese, S., (2014). A Critical Reflection on the Threat from Human Insiders – Its Nature, Industry Perceptions, and Detection Approaches. In: Tryfonas T., Askoxylakis I. (Eds.) Human Aspects of Information Security, Privacy, and Trust. Lecture Notes in Computer Science. Vol 8533. Springer, Cham.

Rashid, T., Agrafiotis, I., and Nurse, J. R.C. (2016). A new take on insider threats: Exploring the use of hidden Markov models. ACM (Eds.) In 8th ACM CCS International Workshop on Managing Insider Security Threats (MIST*)*, Vienna, Austria.

Sasse, M.A., Smith, M., Herley C., Lipford H., and Vaniea K. (2016). Debunking security-usability tradeoff myths. ISBN 1540-7993/16. In IEEE Security and Privacy September/October (pp. 2-8). IEEE Computer and Reliability Societies.

Sasse, M.A., and Smith, M., (2016). The security-usability tradeoff myth. In IEEE Security and Privacy September/October (pp. 11-13). IEEE Computer and Reliability Societies.

Sasse, M.A., (2016) Research Institute in Science of Cyber Security (RISCS). Annual report 2016. University College London.

Widdowson, A.J., Goodliff, P.B (2015). CHEAT, an approach to incorporating human factors in cyber security assessments. In Proceedings of the IET International Conference in Systems Safety and Cyber Security, UK.

Widdowson, A.J., (2016). CHEAT: An updated approach for incorporating human factors in cyber security assessments. Engineering and Technology Reference, 7, 1-7. ISSN 2056-4007.

Williams, J.C. (1986). A proposed method for assessing and reducing human error. In Proceedings of the 9th Advance in Reliability Technology Symposium, University of Bradford (pp. B3/R/1–B3/R/13).