EAI Endorsed Transactions
on Security and Safety

Research Article

Framing the Human Dimension in Cybersecurity

J. Nixon and B. McGuinness*

BAE Systems, Advanced Technology Centre, Filton, Bristol, UK

Abstract

The advent of technologies that can seamlessly operate in different environments with differing levels of security present new challenges to the cybersecurity specialist seeking to ensure the safety of data, process or output of a complex system.

This paper reviews the human dimension of cybersecurity. The Human Factors Integration (HFI) framework is employed as a structure with which to consider the many ways in which the human can differentially affect the security of a system both positively and negatively.

We conclude that when the human factors element is analysed when specifying and designing secure and safe systems, it is far more likely that the human can assist and increase the overall level of security. As in other high technology sectors such as aviation or petrochemical, if not considered, the human can often 'bulldoze' through the most carefully considered and designed security or safety barriers

Keywords: cyber security,cyber safety, cyber warfare, human factors, human factors integration, HFI, human dimension

Received on 27 March 2012; accepted on 27 March 2013, published on 03 May 2013

doi: 10.4108/trans.sesa.01-06.2013.e1

1. Introduction

Barely a week goes by in which a cyber-threat somewhere in the world is not headline news. Moreover, the appearance of such headlines appears to be quickening in pace. The reasons for this rising concern are clear:

(1) The critical infrastructures of society are increasingly dependent on cyberspace, i.e. complex information and communication technology (ICT) networks, public and private, military and civilian, including the Internet.
(2) With greater reliance comes greater vulnerability, and the growing risk of serious, widespread systems failure resulting from deliberate disruption or loss of critical networks.
(3) In contrast to physical attacks, attacks against critical networks or data are relatively cheap and easy to conduct remotely.

Personal communication devices such as mobile phones, or smartphones exacerbate the threat as these devices are so interwoven into everyday life that security is either overlooked or taken for granted. The trend of increasing technology being embedded into everyday life and activities is not likely to abate. The combination of growing threat, growing vulnerability and more serious consequences increases the total risk to national security.

In addition to the technological aspect, the human element in cybersecurity is inherently complex and as such is often vulnerable. At the same time, the implementation of technical security measures can have unforeseen human consequences. Often, a side-effect of implementing a security measure is a reduction of effectiveness or efficiency. Security checkpoints, for example, reduce the flow of people in and out of buildings. Often the technological security of a system is strong but the role and

* Corresponding author. Email: barry.mcguinness@baesystems.com

vulnerabilities of the human in that system are less well understood or considered.

In this paper, we present a broad overview of human factors issues related to cybersecurity. We partition issues in accordance with the Human Factors Integration (HFI) framework. HFI is an integral component of systems engineering for defence capability development in the UK. HFI is a systematic process for identifying, tracking and resolving the wide range of human related issues in the development of capability. The HFI framework has been selected since BAE Systems is mandated to adhere to this standard when working with the UK Ministry of Defence (MoD). The HFI framework is broadly comparable to the Human Systems Integration framework (HSI) used in the United States (Pew and Mavor, 2007; Booher, 2003). The Human Factors themes represented in HFI are consistent with systems engineering and capability development and as such should be included when designing or engineering a system which demands strong cybersecurity in defence applications and elsewhere. Human factors risks and challenges that are identified through application of the HFI process can then be addressed using the appropriate methods, ensuring that the impact of the human on cybersecurity is understood and addressed during the design of a system.

2. Analysis

The HFI framework is used here to structure the human factors issues in cybersecurity. The key mandate of the HFI process is to characterise and address the risks to a system generated by the human. Priority should necessarily be given to the area or areas that present the greatest risk in any given context.

HFI is divided into seven *domains*:

- Social & Organisational Factors
- Manpower
- Personnel
- Human Factors Engineering
- System Safety
- Training
- Health Hazard Assessment

Some domains of the HFI framework are more readily applicable to cybersecurity than others. In this paper the domains of manpower and personnel are combined as the issues raised are complimentary. In addition, Human Factors Engineering and System Safety are combined since the key driver of ‘cybersafety’ is effective use of the equipment by the human operator and a reduction in human error. Health hazard assessment is primarily related to environmental stressors that may cause illness or injury, for example noise, vibration or radioactivity. No specific issues related to cybersecurity were identified in this domain and as such it is excluded from this analysis.

2.1 Social & Organisational Factors

Organisations are a mixture of socio-technical systems, with each component, including each individual, presenting vulnerabilities that are open to accidental or malicious exploitation. Boyce et al. (2011) argue that failure to integrate social factors in cybersecurity development could substantially reduce the effectiveness of cybersecurity capabilities. For example, ineffective management or poor cybersafety culture in an organisation could easily negate the expected benefits of user-centred systems, training, and other areas of HFI.

Malicious attacks by people within the organisation are now considered a bigger threat than external agents (Wilding, 2007; Shaw et al., 1998). However, gaps in the literature have made it difficult for organisations to develop a comprehensive understanding of the insider threat. In particular, there is a need to integrate social psychological and behavioural insights with technical security measures (Kowalski et al., 2008).

One possible approach could be to replicate the US Government-funded Insider Threat Study (ITS). Initiated in 2002, the ITS is a multi-year, multi-disciplinary and cross-sector exploration of employees who have used their organisation’s computer systems or networks to perpetrate acts of harm against the organisation such as theft of intellectual property, fraud or acts of sabotage. ITS is a collaborative initiative of the Secret Service National Threat Assessment Center and Carnegie Mellon University’s Computer Emergency Response Program.

The overall objective of the ITS is to help private industry, government, and law enforcement better understand, detect and prevent harmful insider activity. A particular focus of the study is to identify behavioural precursors and indicators through an annual survey and in-depth case studies looking for statistical patterns (Kowalski et al., 2008).

Many incidents that have involved the release of malware into a network have stemmed from a mis-judgment or error by a user, such as using an unencrypted USB device or violating procedures regarding external email. The existence of appropriate policies, standards and systems does not necessarily mean that cybersecurity will always be correctly implemented. Business process and security solutions are often at odds with each other. An example is credit card online authentication systems which often bombard the user with requests for rarely used, complex passwords making online transactions an inconvenience and often leading a user to engage in unsafe behaviour such as keeping a written record of a password.

The users of a system or service and those who specify it have the responsibility to not only specify the correct standards but also to enforce compliance and ensure correct usage. Moreover, cyber-attackers have regularly penetrated well-designed, secure computer systems by taking

advantage of the carelessness of trusted individuals, or by deliberately deceiving them, for example by pretending to be the system administrator and asking for passwords.

Sasse et al. (2007) highlight a range of social and organisational factors that affect the cultural acceptance of new cybersecurity requirements within an organisation. The imposition by management of tighter restrictions and controls on staff behaviour certainly reduces security risks in the short term but does not necessarily change security awareness and motivation, and may adversely affect the long-term relationship between management and staff. A key message of Sasse et al.'s white paper is that "security is everybody's business." To manage human vulnerabilities effectively, all stakeholders need to be involved in the design and operation of secure systems. It is also essential to communicate effectively about the risks and how to manage them.

At the same time, however, Sasse et al. (2007) acknowledge that there are numerous factors other than security to take into account when considering human behaviour. Trusting a new subcontractor, for example, may be risky in terms of security but highly desirable in terms of business. Similarly, a work environment that imposes draconian security measures can negatively affect employee morale. Hence, the "human factors of cybersecurity" are not just security-specific factors such as handling passwords but also non-security factors that are in turn affected by security. Each organisation must decide its own risk tolerance level, and that may vary from one situation to another.

Human vulnerabilities should ideally be identified and managed before they lead to an actual breach of security. However, according to Sasse et al. (2007), there is currently a tendency to ignore risky human characteristics and behaviours until an actual breach of security occurs.

One solution would be to provide a confidential and anonymous security vulnerability reporting system comparable to those used in high-risk industries to report safety incidents. For example, an individual might report that he observed a colleague's passwords written on a piece of paper. The aim would be to not only react to such vulnerabilities but to share awareness and understanding of them amongst all staff, enabling long-term organisational learning.

At the same time, a confidential reporting system should encourage anonymous whistle-blowing, provided incentives are present for the detection and reporting of possible insider threats by co-workers (DHS, 2009).

Within any organisation, between organisations at a national level, and even between nations at the global level, there is a need for systems to support shared awareness of the cyber domain and its emerging threats. For example, criminal groups and foreign intelligence groups are making increased use of social networking sites such as Facebook (McGannon & Hurley, 2009). Updates on such developments and their implications for ICT users need to be effectively communicated throughout an organisation.

This is a complex problem that must be met collaboratively to provide a comprehensive and integrated response by all stakeholders. This need not require any special or new equipment, just the ability to combine multiple types of information and share appropriately-designed situation briefs, alerts and visualisations based on a combined, continuous intelligence assessment. This requires:

- Improved methodologies for threat, vulnerability, risk and dependency assessment.
- Collaborative information sharing about threats.
- A framework of processes that deliver understanding and situational awareness, all of which is done collaboratively across public and private sectors, at a national and international level.

An explanatory concept that can be used to design for shared awareness and collaboration is that of shared situation awareness and shared mental models (Cannon-Bowers et al., 1993). A mental model is an internalised cognitive representation of a system (Wilson and Rutherford, 1989). Such representations can be invoked by the user to predict future system status or outputs or to comprehend current system status (McGuinness and Dawson, 2005). An effective mental model may be viewed as prerequisite for effective situation awareness. In shared awareness, common or overlapping mental models of a system are required by a group of users. Such models may all be different but support a common goal through co-ordinated tasks. In highly proceduralised environments where users are co-located, such as the flight deck of a commercial airliner, this shared mental model may develop through effective communication and application of procedures.

In cybersecurity effective shared mental models of emerging threats can facilitate safe behaviour and reduce risk. Such a shared mental model of risk presents challenges in this domain. Users may not be co-located or may work for different businesses that are required to interact. For example, employees working for different companies may require shared understanding of when information is commercially sensitive or classified despite differences in their individual tasks or roles. Such geographical and cultural distribution leads to challenges in creating common and overlapping mental models required for all individuals to understand their responsibility to ensure safe 'cyber-behaviour'. As a shared goal, cybersecurity is often secondary to the primary task. Many different tasks can require the same shared mental model to be invoked to ensure safe behaviour. Organisational pressure or cultural differences can change when and how such a model is both created and invoked leading to increased risk of unsafe behaviour. Effective training and human factors analysis which considers these challenges can assist organisations to

overcome such barriers and encourage the generation of appropriate shared mental models. Users can draw upon these shared mental models to reduce the risks presented in the cyber domain though effective decision making.

2.2 Manpower and Personnel

Manpower and personnel efforts focus on the identifying the demand for individual employees (manpower) and the specific competencies that are required (personnel).

Key manpower issues in cybersecurity include meeting the number of personnel required for different roles. Closely tied to this area is the increasing need for outsourcing to meet demand. Key personnel issues in cybersecurity include the specification of knowledge, skills and other attributes required for the different roles.

In the commercial world, one factor that is of special relevance to cybersecurity is the growing demand for outsourcing non-core functions such as data processing, administration and server hosting. A particular concern is outsourcing to overseas suppliers often based in different continents with a variety of governance and oversight structures. Outsourcing presents security issues whether the outsourced activity is cybersecurity itself or other business functions (CPNI, 2009).

Drawing on the BT Group's (formerly British Telecom) overseas outsourcing experience, Colwill and Jones (2007) describe some of the key human factors that can impact significantly on the security of outsourcing. They argue that application of technology alone will not provide solutions. The main requirement for the customer organisation is to ensure or enforce trustworthiness of outsourced personnel through measures such as rigorous employee vetting requirements. This may only be effective in the long term rather than short term – and this in itself presents a major challenge in the outsourcing world which frequently experiences high turnover of personnel.

To ensure effective security in outsourced operations, clear ownership of security is required, as well as a means of instilling in the supplier organisation an understanding of the customer organisation's need for security. New approaches need to be considered for building and maintaining trust and secure relationships between organisations over time.

Although the demand is surging, the supply of suitably qualified cybersecurity professionals is low. Currently in the UK, despite the formation of the Institute of Information Security Professionals in 2006 (BERR, 2008), people are entering the cybersecurity profession through a diversity of routes. One problem is the lack of teachers: qualified experts are needed to teach the next generation of qualified experts. In most cases, cybersecurity is taught as a single module within a Computer Science degree programme. Whereas new legislation may require cybersecurity professionals to be properly certified, the dearth of qualified professionals has even seen agencies looking to students to help fill their positions (Chabrow, 2009).

The Manpower and Personnel domains, then, face several challenges to ensure continuing security:

- The specification of required knowledge, skills and other attributes (both currently and in the future) in cybersecurity professionals.
- The low availability of appropriate candidates for the required roles (both currently and in the future).
- Implementation of effective employee screening to elicit risk factors.
- Understanding and avoiding recruitment of potential or actual internal threats.
- Recruitment or contracting of employees to evaluate vulnerability to external social engineering threats.
- Detection of internal threats among staff.
- Specification and recruitment of emergency cyber response teams.
- Specification of cybersecurity competencies required of ordinary staff.

2.3 Training

Training is a key issue since most often employees are trained in the *how* of cybersecurity but not the *why*. As a result, the *context* of a security procedure or process is not fully understood. One consequence of this is that a user is not able to make reliable risk assessments if workarounds are performed. Employees must feel included in the whole security process and thereby assume a personal responsibility toward maintaining security in the organisation.

U.S. Government research (Noonan & Archeluta, 2008) indicates that many critical infrastructure managers lack an appropriate awareness of the threat that insiders pose. Education and awareness presents the biggest potential remedy by motivating and focusing management efforts to address the insider threat. Training should have the goal of establishing a common baseline understanding of the emerging and dynamic insider threat to critical infrastructures (Noonan & Archeluta, 2008). Research is needed to determine the required content and delivery of such training.

The ISO standards are based in part on the BS 7799 British standards on information security. According to BERR (2008), the globalisation of these standards appears to be helping raise awareness in the UK, at least in certain sectors. Awareness is highest in the financial services, telecommunications, technology and retail sectors; it is weakest in the property, travel, leisure and entertainment sectors. Implementation of the international Information Security Management standards (ISO 27000) is also on the

increase, mainly in the larger companies. Implementation tends to raise the security baseline by ensuring that a minimum level of control is adopted in all areas of security management.

Over time, staff awareness of cyber threats can quickly fade, while the skills for preventing, detecting and responding to attacks can quickly become outdated. At the same time, because cyber-attacks are rarely encountered by individuals, the necessary skills are rarely if ever practiced after initial training. Hence, there is a need for periodic staff assessment and refresher training, not just to update current threat awareness but also to minimise deterioration of security competencies (skill fade). This requirement will differ, of course, for different staff roles and responsibilities. Cybersecurity specialists could be assessed through simulation exercises at six-month intervals in the manner of safety-critical operators such as airline pilots. Other staff could be given monthly awareness updates or even weekly reminders in addition to annual training sessions.

Training Needs Analysis methods provide a framework to evaluate training requirements, matching skills, knowledge and attitudes to tasks. Application of such formal methods is standard within the defence sector. A structured approach to training cybersecurity can clearly identify skills and knowledge gaps, targeting training efficiently to achieve improved cybersecurity.

Frequently, effective application of security processes and procedures require co-operation between groups of individuals in different locations and different companies. The US Air force has developed the concept of Mission Essential Competencies (MECs) (Symons, 2006; Gentner et al. 1999). MECs can be effectively applied to analyse the competencies required by teams to perform a task. Use of MECs in this domain may assist understanding of competencies required for teams, leading to increased threat awareness among groups of individuals.

2.4 Human Factors Engineering and System Safety

Systems designed to help prevent or detect cyber-attacks are critical. However, technical research and development tends to emphasise technological capabilities over human capabilities and with insufficient regard for human limitations. The methods and tools of human factors engineering (HFE) can be used to redress this situation. To be most effective, however, cybersecurity HFE should be integrated into the system development life cycle from system inception. Early integration of human-centric security concerns provides maximum return on investment in cybersecurity.

Human-centric assessment

The degree to which an ICT asset is “secure” can be measured as the extent to which its entire vulnerability to attack is reduced or minimised. However, the cybersecurity field lacks adequate methods to evaluate security and/or vulnerability, especially at the human level. The U.S. Department of Homeland Security identifies enterprise-level cybersecurity metrics as one of the “hard problems” of developing cybersecurity: “Without realistic, precise evaluations, the field cannot gauge its progress toward handling security threats, and system procurement is seriously impeded” (DHS, 2009, p.22)

Effective measurement of human-system interaction is essential when evaluating security processes and procedures. Greater understanding of human perceptions, behaviours and attitudes as users interact with security systems and processes is needed. Such understanding is required to predict the likelihood of users’ acceptance of proposed security measures, whether through models or through human-in-the-loop evaluations. As an example, biometric systems such as iris recognition systems in airports could certainly benefit from a human factors assessment before being deployed in the field.

An analysis of the work which the user is required to perform can greatly assist in understanding how users interact with security systems and processes, enabling human-centric assessment of new and existing technology. In the UK, hierarchical task analysis (HTA) is traditionally used as a starting point for the human factors practitioner to understand the tasks and goals that the user is required to perform (for example, Stammers and Shepard, 2005; Kirwan and Ainsworth, 1992). HTA provides a structured picture of the sequences of tasks that a user performs to achieve a system goal. From this detailed analysis, barriers to performance, weaknesses in the system or procedures can be identified and tasks re-ordered or changed as necessary. The granularity of an HTA can be as fine as is required, allowing the practitioner to examine the interactions of different tasks in great detail.

Task analysis that examines the cognitive work that is required of a user is especially important in complex, socio-technical systems. The security systems and processes often form part of such systems. Understanding the cognitive work which underlies user judgement and decision making is key to developing systems which reduce the risk of a user working around or failing to comply with a process of procedure underlying effective cybersecurity. Cognitive task analysis is a collective term that can be used to understand and articulate user judgements and decision making (Stanton et al. 2004). Examples of specific methods include Cognitive Work Analysis (Vincente, 1999) and Critical Decision Method (Klein and Armstrong, 2004).

Human error and reliability analysis

Unintentional behaviours that create or exacerbate an ICT security vulnerability can be addressed by adapting the methods of human error analysis and human reliability analysis. There are two approaches to human error analysis: at the level of the individual and at the level of the

organisation. The individual level acknowledges the role of the person as an agent with legal responsibilities defined by their contract of employment. As such, an outcome of this level of analysis is often the assignment of blame to the individual concerned. However, it is now widely accepted that individual errors or unsafe-acts do not arise spontaneously and in isolation but in a context of unsafe-preconditions at the system level, such as poor supervision (Shappell and Wiegmann, 2000). Hence, individual error analysis is complemented by analysis at the level of the organisation or system, focusing on aspects such as safety culture and the effectiveness of communication processes. Resilience engineering is an emerging concept which can be applied to understand human error at the organisational level, as opposed to the individual level (Hollnagel et al., 2006). A core dimension of resilience engineering is ensuring that the organisation can respond flexibly and effectively to disruptions. Such flexible response by individuals within an organisation is required when managing and identifying threats which can be varied and unpredictable in the cybersecurity domain.

The individual level of analysis is useful for understanding what specifically happens "at the sharp end" when things go wrong. Human errors can be classified in various ways, such as skill-based, knowledge-based and rule-based. The study of cognitive errors in judgement and decision-making is a particularly rich field, revealing important limitations of everyday cognitive abilities. Although error analysis is retrospective, reliability analysis is prospective. One method for predicting human reliability is probabilistic risk assessment: in the same way that equipment can fail, so can a human user commit security errors. In the human case, task analysis can be used to articulate and quantify the probability of error.

Trust and deception

Trust in a system has the ability to modify user response to that technology (Lee and See, 2004). Trust is defined here as a social response to technology which can guide a user's response when addressing complex, uncertain or unanticipated situations. Nass et al. (1995) have shown that user reactions to computers are similar to those found when users collaborate with other humans. This is relevant in the cybersecurity domain since users may be deceived into performing unsafe actions that exploit their trust in the system (McQueen and Boyer, 2009). Activities that fall into this category include deceiving a user into performing an unsafe act such as downloading and running an executable file or falsifying identity, causing a user to believe they are interacting with someone known to them.

Insufficient and excessive levels of trust in systems have been shown to affect user behaviour. Parasuraman and Riley (1997) characterise these affects as misuse and disuse. Misuse is described as inappropriate levels of reliance on the system indicating a higher than appropriate level of trust. Disuse signifies failures related to the rejection of effective system functionality for example, possibly causing a user to reject a valid e-mail as a phishing attempt This is essentially a mis-calibration of trust. For example, a computerised system can be perceived as infallible since it has been designed to replace or augment more limited human capabilities (Itoh, 2011). In cybersecurity it is possible for users to trust that their protective systems such as firewalls and anti-virus software do indeed prevent attacks when such protection does require a degree of user awareness to be effective. Some apparently 'failsafe' systems, such as biometric access control systems, are still far from reliable. The problem of over-trust is exacerbated by the suppliers' claims and advertising, which imply that the products will ensure security under all circumstances

For example, Williams (2009) identifies Trojans (malware in the guise of legitimate software) as "the number one threat to information security." Sophisticated and rapidly evolving malware development means that Trojans remain very difficult to detect. Yet Williams refers to a test in which a bank of 172 current anti-virus systems failed to detect twenty per cent of known Trojans.

In HFE, a number of ways to address this issue have been developed (Lee & See, 2004). For example, systems can be designed in ways which can elicit appropriate level of trust (Lowrey, 2011; Duez et al., 2006; Yeh and Wickens, 2001; Ockerman, 1999) although this research is still in its early stages and often challenging to apply outside the specific context investigated.

Perception management and deterrence

Underpinned by the constructs of trust and deception is the concept of perception management. One of the functions of security measures in general is to deter any would-be attackers. Thus, while some security measures are designed to be highly covert in order to trap unsuspecting attackers, others are highly visible and obvious. This points to the fact that security and vulnerability invariably have two aspects: actual and perceived (Oscarson, 2007)

While the *actual* security or vulnerability of an asset is an objective fact, the *perceived* level of security does not necessarily correlate and can be manipulated. This complicates our understanding of security (Camp, 2000; Kim and Prabhakar, 2000)

An asset is less likely to be attacked if it is perceived by would-be attackers to be highly secure, even if it is not so secure in actuality. In physical security, a *fake* security measure which offers no objective protection, such as a dummy CCTV camera, may be misperceived by adversaries as an actual security measure, and thereby serve as a deterrent. Creating the illusion of security or invulnerability can, if successful, have the same deterrent effects as investing in actual security measures.

Of course, the potential to misperceive security applies to asset-holders as well as would-be attackers. Asset holders might believe their information or systems to be more secure

than they are, especially given the rate of change of threats. This shows that security measures include not only logical protection but also perception management. This also implies that a measurement of security might have to include separate evaluations of both actual and perceived security.

3. Conclusion

With threats such as cyberwarfare, cyberterrorism and cybercrime ever-present and rapidly evolving in complexity, the process of delivering cybersecurity must likewise evolve rapidly and continually. The UK is taking the cyber-threat to national security very seriously and has begun to commit funds to research and development to address emerging issues and requirements. The HFI framework is a way in which the risks, and indeed benefits, that humans add to the cybersecurity domain can be articulated and addressed.

What is striking about HFI is the breadth of human factors issues and considerations. This breadth can present challenge given time and budget constraints. However, a key function of the HFI process is to examine risks in a structured way. The greatest risks originating from the human factor can be prioritised and acted upon appropriately in accordance with time and budget constraints.

Humans are potentially the greatest strength of cybersecurity (Hernandez, 2010), but only if the human factor is fully considered. For example, it is necessary to consider the trade-offs between the implementation of security measures and the subtle effects of those upon employees' perceptions, motivations, and behaviours. Without taking account of the human dimension in the implementation of security measures, there is an ironic risk of creating and exacerbating human vulnerabilities.

In order for cybersecurity to meet its aims and objectives, the design of systems must match the capabilities and limitations of humans to ensure the highest possible levels of security and safety in the future.

References

[1] BERR (2008) *2008 Information Security Breaches Survey*. Technical Report. Department for Business, Enterprise and Regulatory Reform, April 2008.

[2] BOOHER, H.R. (2003). *Handbook on Human System Integration.* NJ: John Wiley & Sons.

[3] BOYCE, M.W., MUSE-DUMA, K., HETTINGER, L.J., MALONE, T.B., WILSON, D.P., LOCKETT-REYNOLDS, J., (2011). Human performance in cybersecurity: A research agenda. In *Proceedings of the Human Factors and Ergonomics Society 55th Annual Meeting.*

[4] CAMP L J (2000) Trust and Risk in Internet Commerce, MIT Press,Cambridge, MA, USA.

[5] CANNON-BOWERS, J.A, SALAS, E., CONVERSE, S. (1993) Shared Mental Models in Expert Team decision Making In Castellan, N.J. *Individual and Group Decision Making: Current Issues*, LEA, Hillsdale, NJ

[6] CHABROW, E. (2009) Cybersecurity year in review – top 10 happenings. Article in *Bank Information Security*

[7] COLWILL, C. & JONES, A. (2007). The Importance of Human Factors when Assessing Outsourcing Security Risks. Proceedings of the 5th Australian Information Security Management Conference. Edith Cowan University, Perth Western Australia, December 4th

[8] CPNI (2009) *Outsourcing: Security Governance Framework for IT Managed Servive Provision*. Good Practice Guide – 2nd Edition. Centre for the Protection of National Infrastructure.

[9] DHS (2009) *A Roadmap for Cybersecurity Research*. U.S. Department of Homeland Security, Science and Technology Directorate, November 2009.

[10] DUEZ, P. P., ZULIANI, M. J. & JAMIESON, G. A. (2006) Trust by design: Information requirements for appropriate trust in automation. *Proceedings of the 2006 conference of the Centre for Advanced Studies on Collaborative Research.*

[11] GENTNER, F. C., TILLER, T.C., CUNNINGHAM ,P. H., BENNETT, W. (1999) Using Mission Essential MOEs/MOPs for Evaluating Effectiveness of Distributed Mission. *Training Proceedings of the Interservice/ Industry Training, Simulation & Education Conference (I/ITSEC) 1999.*

[12] HERNANDEZ, J. (2010) The human element complicates cybersecurity. Defense Systems website (defense systems,.com), 2 March 2010.

[13] HOLLNAGEL, E., WOODS, D.D., LEVESON, N. (2006). *Resilience Engineering.* Ashgate.

[14] ITOH, M. (2011) A model of trust in automation: Why humans over-trust? *Proceedings of SICE Annual Conference*, Tokyo, 13-18 Sept 2011, pp.198-201.

[15] KIM K AND PRABHAKAR B (2000) Initial Trust, Perceived Risk, and the Adoption of Internet Banking, *In Proceedings of the Twenty-First International Conference on Information Systems (ICIS 2000)*,December 10–13, 2000, Brisbane, Australia.

[16] KIRWAN, B., AINSWORTH, L. K. (1992) *A Guide to Task Analysis*. Taylor and Francis. London, UK

[17] KLEIN, G., & ARMSTRONG, A. A. (2004). Critical decision method. In N. Stanton, A. Hedge, K. Brookhuis, E. Salas & H. Hendrick (Eds.), *Handbook of human factors and ergonomics methods*. CRC Press. London, UK

[18] KOWALSKI, E., CAPPELLI, D. & MOORE, A. (2008) Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector. Carnegi Mellon Software Engineering Institute.

[19] LEE, J. D. & SEE, K. A. (2004) Trust in Automation: Designing for Appropriate Reliance. *Human Factors*, 46, 50-80.

[20] LOWREY, A. (2011). First Impressions Count: The Impact of Visual Attractiveness on User Trust in Computer Decision Aids. Unpublished MSc Thesis, University of Derby.UK

[21] MCGANNON, M. & HURLEY, D. (2009) The dark side of social networking. *IO Sphere*, Summer 2009. Joint Information Operations Warfare Command (JIOWC), San Antonio, Texas.

[22] MCGUINNESS, B., DAWSON, D. (2005) Assessing situational awareness in teams. In Bust, P. D. and McCabe, P. T. (Eds) *Contemporary Ergonomics*. Taylor and Francis. UK.

[23] MCQUEEN, M.A. AND BOYER, W. F. (2009) Deception used for cyber defense of control systems *In proceedings of Human System Interactions*, 21-23 May 2009.

[24] NASS, C., & MOON, Y., FOGG, B. J., REEVES, B., & DRYER, D. C. (1995). Can computer personalities be human

personalities? International *Journal of Human-Computer Studies*, 43, pp. 223-239.

[25] NOONAN, T. & ARCHELUTA, E. (2008) The National Infrastructure Advisory Council's Final Report and Recommendations on The Insider Threat to Critical Infrastructures. NIAC, U.S. Department of Homeland Security.

[26] OCKERMAN, J. J. (1999). Over-reliance issues with task-guidance systems. *In Proceedings of the Human Factors and Ergonomics Society 43rd Annual Meeting* (pp. 1192 – 1196). Santa Monica, CA: Human Factors and Ergonomics Society.

[27] OSCARSON, P. (2007) Actual and Perceived Information Systems Security. Unpublished PhD Thesis, Linköping University, Department of Management and Engineering, Sweden.

[28] PARASURAMAN, R., & RILEY, V. A. (1997) Humans and automation: Use, misuse, disuse, abuse. *Human Factors*, 39(2), pp. 230–253.

[29] PEW, R. W., & MAVOR, A. S. (2007). *Human-System Integration in the System Development Process: A New Look.* Washington, DC: National Academies Press.

[30] SASSE, M. A., ASHENDEN, D., LAWRECE, D., COLES-KEMP, L., FLÉCHAIS, I. & KEARNEY, P. (2007) Human vulnerabilities in Human Factors Working Group White Paper. DTI Cyber Security Knowledge Transfer Network

[31] SHAPPEL, S A & WEIGMANN. D A, (2000) The Human Factors Analysis and Classification System – *HFACS. US Department of Transportation, FAA*, DOT/FAA/AM-00/7

[32] SHAW, E., RUBY, K. G. & POST, J. M. (1998) The insider threat to information systems: The psychology of the dangerous insider. *Security Awareness Bulletin*, 2, 1-10.

[33] STAMMERS, R. B., SHEPHARD, A. (2005) Task Analysis In Wilson, J. R. and Corlett, E. N. (Eds) *Evaluation of Human Work*, Taylor and Francis. UK.

[34] STANTON, N., A., SALMON, P. M., WALKER, G. H., BABER, C., JENKINS, D. P. (2005) *Human Factors Methods*. Ashgate, London UK.

[35] SYMONS, S., FRANCE, M., BELL, J., BENNETT, W. (2006) Linking Knowledge and Skills to Mission Essential Competency-Based Syllabus Development for Distributed Mission Operations Air Force Research Laboratory, Report AFRL-HE-AZ-TR-2006-0041.

[36] VICENTE, K., J. (1999) *Cognitive Work Analysis*, LEA, London

[37] WILDING, R, (2007) Insiders are the biggest enemy, *Strategic Risk*, September 2007.

[38] WILLIAMS, P. (2009) Top 5 Information Security Threats. *API 4th Annual IT Security Conference*, Houston, Texas, 11-12 Nov 2009.

[39] WILSON, J. R & RUTHERFORD A., (1989). Wilson, J. R., & Rutherford, A. (1989) Mental models: Theory and application in human factors. *Human Factors*, 31, 6, 617-634.

[40] YEH, M., & WICKENS, C. D. (2001). Display signalling in augmented reality: Effects of cue reliability and image realism on attention allocation and trust calibration. *Human Factors*, 43, pp. 355 – 365.