Trends in Information Management (TRIM)
ISSN: 0973-4163
14(1), pp. 1-15

Causes of Human Errors in Information Security: A Grounded Theory Study

M. Ahmed
L. Sharif
F. Ahmed

Abstract

In this paper, the role of human errors in the field of information security is discussed. The latter has attracted much attention from information security researchers in the recent past. According to current statistics, human errors are a major component of problems in information security, with 68% of breaches involving a non-malicious human element (Verizon Business, 2024) and the global average cost of a data breach reaching $4.88 million (IBM, 2024). In spite of such alarming statistics, there has been comparatively little empirical research on the role of human errors in information security. This is particularly evident at organizational level, due in large part to the unwillingness of organizations to share information and statistics on security issues. In this paper, grounded theory has been employed as a research methodology to investigate the main causes of human errors in information security.

Information security experts (103 in total) from around the globe were asked a series of open-ended questions and their responses were used to develop a detailed list of human errors. This paper represents an important contribution to our understanding of the causes of human error in information security.

Keywords: *Grounded Theory, Human Errors, Human Computer Interaction, Information Security, Structural Equation Modelling, Security Engineering*

Introduction

Security breaches have escalated sharply in recent years, inflicting substantial financial and reputational losses on the organizations affected. This trend has brought information security to the forefront of attention across industry, government, and academia.

The discipline rests on three core principles — confidentiality, integrity, and availability (SANS Institute, 2024; Stallings & Brown, 2023) — upheld through the complementary techniques of prevention, detection, and response (Dhillon & Backhouse, 2001; Von Solms & Van Niekerk, 2013). Underpinning all three is the capacity to distinguish authorized from unauthorized users, a process known as user authentication, regardless of whether a user connects from the workplace, from home, or from any other location.

The information security research community has increasingly acknowledged the part that human behaviour plays in security failures. In spite of many advances in security technology, humans remain widely regarded as the weakest link in the security chain, and the contribution of human factors to security breaches is still inadequately addressed by prevailing models. Researchers and practitioners have repeatedly urged that human factors be woven into the design and evaluation of IT security systems

(Khadka & Ullah, 2025). Human–Computer Interaction (HCI), a discipline that places the human dimension at the centre of system design, offers a relevant perspective: it pursues an optimal trade-off between the quality of system output and the cost — to users, stakeholders, and the system itself — of achieving it. Yan et al. (2017) and McNeese and Forster (2017) have argued that HCI research should develop validated theory and models so that practical knowledge can be transferred more reliably to new designs.

Information security has traditionally been seen as a technical challenge — a matter of hardware and software. Yet research has shown that an overwhelming share of breaches stems from human factors such as inadequate training and limited security awareness (Ahmed, 2013). Many organizations still direct their efforts almost entirely toward technological controls, overlooking the human dimension. Technical safeguards are indispensable, but on their own they cannot compensate for the errors and oversights of the people who use IT systems. Discussion of new threats within the security community, although valuable, does not automatically translate into better-informed end users (ISO/IEC 27001:2022).

Human errors in the field of information technology and security cause great losses around the world. In May 2017, British Airways suffered a major IT outage widely attributed to human error when a contractor accidentally powered down and then restarted the uninterruptible power supply at a data center. This prevented the booking and boarding of flights throughout the day as well as missing luggage for passengers and financial losses estimated at over £80 million for the airline. Additionally, the misuse of passwords in business systems and highly important sites makes these sites easy targets for intruders on the Internet. Research has consistently highlighted the need for clear policies to change passwords periodically and for passwords to be complex and strong enough to protect systems from hacking or session hijacking (NCSC, 2024).

More recently, a discussion on human errors was sparked by the revelation that drug errors in England have been causing appalling levels of harm and death. Research carried out by researchers from Manchester, Sheffield and York universities suggested that 237 million drug-related errors were being made in GPs, hospitals, pharmacies and care homes which amounted to 700 deaths a year. Janet Davies, the chief executive of the Royal College of Nursing concluded that human error was one of the biggest risks in medicine, whereas Secretary Jeremy Hunt pointed out that human error was a global phenomenon and not unique to one country. It is evident that human error is a predominant cause of crime/cybercrime, affecting companies and institutions from all areas alike (Elliott et al., 2018).

Related Work

Within parts of the information security industry there has long been a

tendency to treat technology as a complete answer to security problems.

Yet technical controls cannot, on their own, manage the full range of security risks; the people within an organization remain its first line of defence (Abdulla et al., 2014; NCSC, 2024). Tools such as firewalls, antivirus software, and virtual private networks (VPNs) are undeniably important elements of an organization's defensive arsenal, but relying on a purely technological strategy carries serious limitations.

Ultimately, information security is a human matter. Studies of how attackers compromise IT systems repeatedly show that the human element is decisive in most successful intrusions. A careless employee's simple misconfiguration can leave network ports exposed, weaken firewalls, and render entire systems defenceless. In practice, human error is a more probable cause of serious breaches than technical weaknesses alone (Hadlington, 2021; Verizon Business, 2024).

Empirical investigation of human error in information security nonetheless remains limited, particularly at the organizational level (Pollock, 2017; Sulaiman et al., 2022), although recent interdisciplinary research has begun to close this gap (Khadka & Ullah, 2025). The scarcity of evidence is widely attributed to organizations' reluctance to disclose data on their security incidents and vulnerabilities. This reticence is consequential, since the continued growth of the internet and e-commerce depends on understanding and reducing such errors.

The prominence of human error is not unique to computing. Across high-risk industries — from aviation to nuclear power generation — human error is estimated to account for the majority of recorded events, with figures commonly cited at around 80 percent and higher (U.S. Department of Energy, 2009). Human and technological factors cannot be cleanly separated, because accomplishing almost any task today depends on both.

Few occupations now operate without technology, yet machines lack human intuition and judgment and must be instructed through explicit commands. While an operator can interpret machine feedback such as alarms and readings and translate it into new instructions, full automation has not displaced this human role: Airbus's attempt to introduce fully automated airliners, for instance, was rejected by the travelling public. Interaction between people and machines is therefore enduring (Shneiderman et al., 2022).

Because every failure can ultimately be traced to a human decision somewhere in the chain, people tend to seek someone to hold responsible when things go wrong.

Human cognition is intricate and shaped by numerous influences, which may be grouped as internal — those arising from the organizational environment — and external, relating to an individual's personal life. As humans are inherently fallible, error can never be wholly eliminated (Pascoe et al., 2024).

The contributing factors are many and include inadequate supervision, carelessness, lapses in concentration, and insufficient training; depending on the setting, the resulting errors may be severe enough that they cannot be discounted in any serious risk assessment.

Consistent with this, human factors research continues to characterize people as the weakest link in the security chain (Khadka & Ullah, 2025). Contemporary industry reporting bears this out: the 2024 Data Breach Investigations Report found that a non-malicious human element — error or social engineering — was a component of 68 percent of breaches, with errors alone implicated in 28 percent (Verizon Business, 2024). Table 1 sets out these and other leading factors. Analyses of breach costs similarly underline the financial weight of the human factor (IBM, 2024), and comparable work has likewise reported that a substantial share of incidents stem from human error rather than deliberate crime (Ahmed et al., 2012; Harper et al., 2015).

Table 1: Selected contributing factors in data breaches; categories overlap and do not sum to 100%. Adapted from Verizon Business (2024)

Contributing factor	Breaches (%)
Human element (non-malicious: error or social engineering)	68
Errors	28
Ransomware and other extortion	32
Third-party involvement	15

Although a considerable body of statistics documents the prevalence of human error in organizational settings, far less attention has been paid to techniques for reducing or mitigating it.

Reason's Generic Error Modelling System

Preventing human error in information security depends first on recognizing the different forms such error takes, alerting users to the associated risks, and putting measures in place to forestall them. The human factors field has produced a range of models for understanding and classifying types and levels of human error, and these have been applied successfully across industries to investigate the causes of accidents (Reason, 1990). Among them, the Generic Error Modelling System (GEMS) examines both the cognitive mechanisms underlying error and the organizational and managerial conditions that make error more likely (Reason, 1990; Reason, 1997). GEMS offers a useful lens for interpreting human error in information security.

Under GEMS, mental activity operates in one of two modes (Reason, 1990):

- *Attentional Mode:* draws on conscious awareness and working memory. It is effortful, slow, and hard to sustain over long periods, and it supports tasks such as setting goals, tracking progress, and recovering from

mistakes. In a security context, a user might rely on it when trying to recall login credentials such as a username or password.

- *Schematic Control Mode:* handles familiar information rapidly and with little conscious effort, and is not constrained by the volume or duration of the information held.

Different types and levels of error can arise at the various stages of cognitive processing.

Categories of Behaviour for Distinguishing Error Types

Reason (1990) classifies human error according to an individual's level of performance.

These errors can be distinguished by both psychological and situational factors, and arise as follows:

- *Skill-based Errors:* are routine, automatic, and unconscious, occurring in schematic control mode; they take the form of slips and lapses — unintended actions.
- *Rule-based Errors:* arise when stored rules are selected and applied to a situation. This behaviour is largely automatic and comes into play when the routine, skill-based response must be adjusted, with the user applying a remembered rule and monitoring its outcome.
- *Knowledge-based Errors:* occur under attentional control and operate from first principles, arising only after a familiar approach has repeatedly failed and no ready-made solution exists.

Most errors tend to be skill-based rather than rule- or knowledge-based.

A further distinction, drawn by the National Research Council's Computer Science and Telecommunications Board, separates accidental from deliberate human error (National Research Council, 2002). Accidental causes are unintentional — a coding mistake that crashes a system, for example — whereas deliberate causes are attacks in which harm is intended. In this paper, human error is taken to cover both.

The errors users commit can open the door to security breaches in several ways, whether through limited technical knowledge, technical mistakes, or plain carelessness. Stanton et al. (2005) set out five categories of end-user security behaviour, spanning users who are both aware and conscientious through to those who deliberately bypass controls; this taxonomy informs how human errors are classified in the present study.

As internet access has become near-universal, many users possess only rudimentary computing skills — enough to browse the web or send email — and remain unaware of the importance of safeguards such as antivirus software, firewalls, and timely updates and patches (Hadlington, 2017). Such users are readily targeted by malware and attackers, and a single compromised machine can become a staging point for attacks on other systems.

Even highly skilled software developers can make consequential mistakes.

Though usually unintentional, these can introduce security loopholes that attackers exploit to seize control of affected systems. Such flaws can be remedied through patches, but administrators and end users do not always apply even critical updates, often through negligence.

Carelessness is among the most common and damaging sources of human error in this domain. It surfaces in many ways — passwords left on visible notes, harmful websites visited despite browser warnings, and security policies disregarded or unenforced. The deliberate omission of security measures has been shown to be strongly predicted by users' attitudes and their perception of threat (Workman et al., 2008).

Weak, easily guessed passwords are another manifestation. An analysis by the UK's National Cyber Security Centre identified "123456" as the most common password found on breached accounts, alongside other predictable choices such as the names of football clubs (NCSC, 2019). Adams and Sasse (1999) argued that users often adopt weak passwords not from ignorance but because security mechanisms fail to fit their needs — an observation that remains pertinent — and the NCSC has described choosing a strong password as the single most important step a user can take for their own online security (NCSC, 2019).

A widely cited demonstration of careless behaviour was an experiment by the U.S. Department of Homeland Security examining how easily attackers might exploit employees to reach internal systems (Edwards et al., 2011). Discs and USB drives were deliberately left in the car parks of government and contractor sites; of those who picked them up, around 60 percent connected the devices to office computers, rising to roughly 90 percent when the device carried an official-looking logo.

Careless or untrained insiders pose an even greater risk. This group includes employees susceptible to social engineering as well as malicious or disaffected staff. The financial toll of breaches is heavy, and most trace back to human error; despite investment in physical and software defences, most organizations remain exposed to even basic risks (Pascoe et al., 2024). A measured combination of policy, procedure, training, and technology offers the best prospect of reducing that exposure.

Research Methodology

Grounded theory (GT) can be defined as a systematic methodology that involves the generation of theory from data (Corbin & Strauss, 2015; Martin & Turner, 1986). Although GT is mainly used in qualitative research, it can quite easily be employed for quantitative data (Corbin & Strauss, 2015; Glaser & Strauss, 1967). GT fundamentally contradicts the conventional model of research. GT works in almost the reverse of conventional research. The process starts with data collection through a selection of methods. Using the collected data, key points are selected using a series of codes derived from

the text. The codes are then grouped into related concepts in order to make them more workable. The concepts form the basis for categories. The latter then form the basis for the creation of theory. The entire process from codes to theory is summarized in Table 2 (Martin & Turner, 1986).

Table 2: Four Stages of Analysis; Adapted from Martin and Turner (1986)

Stage	Purpose
Codes	Identifying anchors that allow the key points of the data to be gathered
Concepts	Collections of codes of similar content that allows the data to be grouped
Categories	Broad groups of similar concepts that are used to generate a theory
Theory	A collection of explanations that explain the subject of the research

Table 3 presents a comparison of some important research methodologies and highlights some of the key features that distinguish GT as a strong candidate for this research:

Table 3: Comparison of Research Methodologies [Adapted from (Creswell & Poth, 2018)]

Dimension	Phenomenology	Grounded Theory	Experiments
Focus	Understanding the essence of experience about a phenomenon	Developing a theory grounded in data from the field	Experiment consists of a planned action
Origin	Philosophy, sociology, psychology	Sociology (we will apply it to engineering field)	Can apply to any field
Data collection	Long interviews with up to 10 people	Interviews with 20–30 individuals to 'saturate' categories and detail a theory	Applied on live computer system
Data analysis	▪ Statements ▪ Meanings ▪ Meaning themes ▪ General description of the experience	▪ Open coding ▪ Axial coding ▪ Selective coding ▪ Conditional matrix	Results are recorded and analyzed or reflected on
Narrative form	Description of the 'essence' of the experience	Theory or theoretical model	Mathematical modelling

Data Collection

The use of open-ended questions in this research allowed the participants to answer questions in an unconstrained manner. Open-ended questions also

allow for finer details to be incorporated to the satisfaction of the participants (Creswell & Poth, 2018) and thus are deemed more suitable for this research as compared to other data gathering techniques such as interviews, questionnaires and experiments (Lazar et al., 2017).

A survey was conducted using open-ended questions in order to find a minimum of five of the most important causes of information security human errors (HE) facing organizations around the world today. Participants were able to answer the open-ended questions using a Word-processed form designed with ample space for both a short title and a detailed rationale for each issue. The forms were pre-tested by two academics from among the sample of information security experts. All were requested to return useable responses.

Table 4 presents a summary of the data collection process. A wide range of geographical regions were represented, as shown in Tables 5 and 6. The respondent pool was 29 countries with academic and industry participation reflective of the types of organizations that hire information security academics and professionals. Tables 5 and 6 list the demographic features of the samples and also show the total numbers: AISE participant numbered 72 and IISEs 31, from 27 and 7 different countries respectively.

Table 4: 103 Participant sent responses

Email sent to participants	No. of participants	Response received from no. of participants	Sampling type
Academics	297	25	Cluster
Academics and Industrial	728	58	Random
First reminder to academics	211	3	Cluster
Second reminder to academics	211	5	Cluster
First reminder to Industrial	123	12	Random
Total	**1025**	**103**	

PhD	= 40
PhD Scholars with MCSE and CCSE	= 28
MSc with MCSE and CCNP	= 4
PhD with CCSE	= 4
PhD Scholars with CCSE	= 14
MSc with MCSE and CCNP	= 4
BSc with MCP and CCNA	= 9

Table 5. Academic Information Security Experts (AISEs) – Participants from 27 Countries

Country	Frequency	Country	Frequency	Country	Frequency
Afghanistan	2	China	3	Palestine	2
Algeria	2	Croatia	2	Saudi Arabia	4
Australia	1	Egypt	4	South Korea	1
Bahrain	2	France	2	Switzerland	1
Bangladesh	1	Italy	2	Syria	1
Bolivia	2	Jamaica	1	Tanzania	1
Bosnia	2	India	4	Thailand	1
Bulgaria	1	Pakistan	5	UK	17
Canada	2	Motswana	1	USA	5

Table 6: Industrial Information Security Experts (IISEs) – Participants from 7 Countries

Country	Frequency	Country	Frequency
Algeria	3	USA	4
Australia	2	India	4
Egypt	4	UK	11
Ghana	3	**Total**	**31**

Data Analysis and Results

This section discusses the data analysis approach that is based on the open coding technique used within GT. Open coding is a technique that employs a form of content analysis in order to classify data into concepts that originate from the data rather than from any pre-defined hypotheses based on outside sources such as literature. The respondents' short titles (i.e. HE causes) as well as a frequency analysis of keywords and phrases in the respondents' rationales form the primary bases for category identification at this stage of coding (Corbin & Strauss, 2015).

The open-ended questions generated 2,060 comments and statements. The total responses contained in excess of 111,240 words, thereby offering rich content that is suitable for qualitative analysis and subsequent development of a theoretical model for this research (to be presented in a future paper).

The above discussion can be summarized in the form of mathematical calculations as follows. The total number of comments/statements in the open-ended questions (Ct) was determined. The participants were asked to provide five HE causes/issues in the first open-ended question. Although the minimum requirement was five HE issues/causes, most participants provided more than two pages of text by listing five or more issues/causes with an explanation of each. Therefore, on average, each participant provided 10 comments or statements.

Total number of participants, Pt	= 103
Average number of comments or statements per participant, Cv	= 10
Total number of comments or statements, Ctq1 = Pt * Cv = 103 * 10	= 1,030
Average number of text pages per participant, Tp	= 2.25
Average number of words per page with single line space, Wp	= 480
Total number of words, Wt = Pt * Tp * Wp = 103 x 2.25 x 480	= 111,240

Using this open coding procedure, 95 categories of causes/issues were identified from the data. The first 20 (of the 95) causes are listed in Table 7.

Table 7: Causes of information security human errors, Top 20 categories after open coding listed in frequency order

S.No.	Causes	Frequency
1	Carelessness and ignorance of employees and users	65
2	Unawareness of common computer knowledge and needs	64
3	Weak password management	54
4	Protection and security issues	43
5	Lack of following policies and structures	34
6	Inexperience and untrained employees	31
7	Cultural issues	25
8	Lazy and uninterested employees and users	23
9	Lack of training and education	22
10	Weak management and leadership	22
11	Technical error by programmers	21
12	Human memory	20
13	Lack of higher management commitment	19
14	Fatigue and stress	17
15	Lack of involvement and motivation	17
16	Viruses and anti-virus ignorance	16
17	Human computer interaction	14
18	Updates and patches	14
19	Behaviour and ethics	14
20	Criminal intent	13

Discussion

As is evident from Table 4, different sampling methods were employed for data collection. Cluster sampling was used for participants known to the authors either directly or indirectly, random sampling for participants unknown to the authors and snowball sampling used for communication among participants. The use of cluster sampling yielded 33 participant responses whilst 70 participant responses resulted from the use of snowball and random sampling. GT stipulates that one full cycle of open, axial and selective coding should be carried out with a set of data before moving to the next phase of this or any other study. The minimum of one hundred participants must also be ISEs, as planned in this research. The originators

go so far as to suggest that researchers should not collect the next set of data until they analyze the previous set. The reason for this is so as to use the learning from coding the set in the next stage. However, it was not possible to collect data from a sufficient number of ISEs. Consequently, the study shifted back and forth between Straussian and Glaserian approaches in order to collect data from a sufficient number of participants. The use of both GT approaches (Straussian and Glaserian) along with the three types of sampling (cluster, random and snowball) was deemed to be the only feasible option. Data were collected from 103 participants by contacting AISEs and IISEs around the world. In total, 1,025 potential participants were contacted, resulting in a 10.04% response rate. Without blending the two GT approaches, it would not have been possible to collect the required data for this research (Pollock, 2017).

As reported by the research participants (see Table 7), user carelessness was ranked as the leading cause of human errors in information security. A lack of computer security knowledge is shown to be the second major cause of human errors in Information Security. Poor password management and a lack/absence of security policy implementation are also deemed to be critical causes of human errors.

Some of the other causes of human errors in information security identified in this research include inexperienced and untrained users, cultural issues, lazy and uninterested employees and users, lack of continuous user training and education, lack of strategic leadership, technical errors by programmers, lack of management commitment, ignorance of computer viruses and outright criminal intent.

The research also suggests that due to global demand, it is a great challenge to recruit and retain adequately trained and educated information security staff.

Conclusions

This paper is an extension of our past work (Ahmed et al., 2012) and an attempt to narrow the gap between the theoretical and practical aspects of information security. In Ahmed et al. (2012), the role of human errors was discussed based on relevant literature in the field. For the purpose of this paper, information security experts from around the world were invited to share their knowledge and expertise in the field. This paper is one of the first information security research studies of its kind to utilize a blended approach based on both Straussian and Glaserian GT techniques. As such, this paper represents a significant contribution to the field.

Future Work

Future work in this field will extend this research by:

1) posing another open-ended question to seek the remedies for human

errors in information security, and

2) using the responses to develop a theoretical model using GT and to derive a survey tool for further data gathering from ISEs to test the theoretical model. The model will be tested for validity using Structural Equation Modelling (SEM).

Acknowledgements

This research has been supervised by Dr. Margaret Volante and critically commented on by Professor Peter Smith at Middlesex University, London, UK.

References

Abdulla, S., Ramadass, S., Altaher, A., & Nassiri, A. (2014). Employing machine learning algorithms to detect unknown scanning and email worms. *The International Arab Journal of Information Technology*, 11(2), 140–148.

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM,* 42(12), 40–46. https://doi.org/10.1145/322796.322806

Ahmed, M. (2013). *Feasibility of an information security human error reduction (ISec-HER) model* [Unpublished doctoral dissertation]. Middlesex University.

Ahmed, M., Sharif, L., Kabir, M., & Almaimani, M. (2012). Human errors in information security. *International Journal of Advanced Trends in Computer Science and Engineering*, 1(3), 82–87.

Corbin, J., & Strauss, A. (2015). *Basics of qualitative research: Techniques and procedures for developing grounded theory* (4th ed.). Sage Publications.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). Sage Publications.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organisational perspectives. *Information Systems Journal*, 11, 127–153.

Edwards, C., Kharif, O., & Riley, M. (2011, June 27). *Human errors fuel hacking as test shows nothing stops idiocy*. Bloomberg.

Elliott, R., Camacho, E., Campbell, F., Jankovic, D., St James, M. M., Kaltenthaler, E., & Faria, R. (2018). Prevalence and economic burden of medication errors in the NHS in England. *Policy Research Unit in Economic Evaluation of Health and Care Interventions (EEPRU)*, University of Sheffield.

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. Aldine.

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards

cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hadlington, L. (2021). The "human factor" in cybersecurity: Exploring the accidental insider. In A. Attrill-Smith, C. Fullwood, M. Keep, & D. J. Kuss (Eds.), *The Oxford handbook of cyberpsychology* (pp. 527–542). Oxford University Press.

Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G., & Williams, T. (2015). *Gray hat hacking: The ethical hacker's handbook* (4th ed.). McGraw Hill.

IBM (2024). Cost of a data breach report 2024. *Ponemon Institute/IBM*. https://www.ibm.com/reports/data-breach

International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC Standard No. 27001:2022). https://www.iso.org/standard/82875.html

Khadka, K., & Ullah, A. B. (2025). Human Factors in Cybersecurity: Understanding the Weakest Link. *Journal of Information Security and Applications,* 89, 103945.

Lazar, J., Feng, J. H., & Hochheiser, H. (2017). *Research methods in human-computer interaction* (2nd ed.). Morgan Kaufmann.

Martin, P., & Turner, B. (1986). *Grounded theory and organizational research*. The Journal of Applied Behavioral Science, 22(2), 141–157.

McNeese, M. D., & Forster, P. K. (2017). *Cognitive systems engineering: An integrative living laboratory framework*. CRC Press.

National Cyber Security Centre. (2019). The UK cyber survey 2019. https://www.ncsc.gov.uk/report/uk-cyber-survey-2019

National Cyber Security Centre. (2024). *Annual review 2024*. https://www.ncsc.gov.uk/collection/ncsc-annual-review-2024

National Research Council. (2002). *Cybersecurity today and tomorrow: Pay now or pay later*. National Academies Press. https://doi.org/10.17226/10274

Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST cybersecurity framework (CSF) 2.0. *National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.CSWP.29

Pollock, T. (2017). Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS). *KSU Conference on Cybersecurity Education, Research and Practice*.

Reason, J. (1990). *Human error*. Cambridge University Press.

Reason, J. (1997). *Managing the risks of organizational accidents*. Ashgate.

SANS Institute. (2024). *Security awareness report 2024*. https://www.sans.org/security-awareness-training/reports/

Shneiderman, B., Plaisant, C., Cohen, M., Jacobs, S., & Elmqvist, N. (2022). *Designing the user interface: Strategies for effective human-computer interaction (6th ed.).* Pearson.

Stallings, W., & Brown, L. (2023). *Computer security: Principles and practice* (5th ed.). Pearson.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, 24(2), 124–133. https://doi.org/10.1016/j.cose.2004.07.001

Sulaiman, N. S., Fauzi, M. A., Wider, W., Rajadurai, J., Hussain, S., & Harun, S. A. (2022). Cyber-information security compliance and violation behaviour in organisations: A systematic review. *Social Sciences (Basel)*, 11(9), 386. https://doi.org/10.3390/socsci11090386

U.S. Department of Energy. (2009). *Human performance improvement handbook: Concepts and principles* (Vol. 1, DOE-HDBK-1028-2009). U.S. Department of Energy.

Verizon Business. (2024). 2024 data breach investigations report (DBIR). Verizon. https://www.verizon.com/business/resources/reports/dbir/

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.006

Yan, Z., Molva, R., Mazurczyk, W., & Kantola, R. (Eds.). (2017). Network and system security: *11th International Conference, NSS 2017, Helsinki, Finland, August 21–23, 2017, proceedings*. Springer.

Corresponding Author

Prof. Munir Ahmed can be contacted at: munir_ahmed@outlook.com

Author Biographies

Prof. Munir Ahmed is the CEO & Consultant Professor, Munir Ahmed Academy, London, United Kingdom & Lecturer in Physics, Leyton Sixth Form College, London, United Kingdon. He has undertaken advanced training in Mixed Methods Research at the University of Oxford and holds double doctorates, double master's degrees, and double undergraduate degrees in Electrical Engineering and Security Engineering, including a Doctorate in Computer Communications Engineering (Information Security) from Middlesex University London. In recent years, he has also contributed to interdisciplinary medical and healthcare publications and is particularly interested in extending his doctoral research on human factors and human

error reduction into medicine and healthcare. With more than 40 years of international experience in academia, industry, research, and consultancy across the United Kingdom, Saudi Arabia, Belgium, Germany, Ireland, and Pakistan, he is currently working as CEO and Consultant Professor for Munir Ahmed Academy London, and Lecturer in Physics for Leyton Sixth Form College, London, United Kingdom. He has also recently taught Mathematics at Newham Sixth Form College and Newham College for Further Education, London.

Professor Ahmed has previously served as Professor of Computer Networks and Security Engineering at Taibah University and Northern Borders University, Saudi Arabia, and as a Senior Research Scholar at Middlesex University London, the University of Greenwich, and London South Bank University. His research interests focus on human factors in information security, human error reduction, medical education, wireless sensor networks, and research methods.

He has authored and co-authored several books and more than 250 scholarly and professional contributions, including journal articles, conference papers, technical manuals, workshops, and industry presentations.

Dr. Lukman Sharif holds a Doctorate in Computer Communications Engineering (Information Security) from Middlesex University London and is a member of the Institution of Engineering and Technology (IET). He works as a Principal Consultant and Researcher, bringing extensive experience in information security, data privacy, and risk management. His research interests span information security, data privacy, AI governance, AI ethics, and responsible AI. He has authored scholarly contributions in the areas of information security, human error, and security training and awareness.

Fatimah Ahmed holds a BA in English Language and Literature from King's College London, where she is currently pursuing her postgraduate studies and teaching English at a grammar school in London. She works as a Lecturer at MA Educational Consultants, London, United Kingdom. Her research interests include human error, human psychology, and human-computer interaction.