International Journal of Computer and Organization Trends
ISSN: 2249 – 2593 / https://doi.org/10.14445/22492593/IJCOT-V16I1P304

Volume 16 Issue 1, 25-31, Jan-Apr 2026


*Original Article*

# A Comprehensive Review Study of Cyber Security and Human-Centred Threat: Non-Malicious Threat within an Organization

Kultar Singh

*Computergesteuerter Versandprozessmanager (Ausgangsprozessmanager), Versand Abteilung, Clic – Trade Gmbh, Cologne, NRW, Deutschland.*

*Corresponding Author : Kultarsingh355@gmail.com*

Received: 13 February 2026 Revised: 16 March 2026 Accepted: 12 April 2026 Published: 30 April 2026

***Abstract -*** *The issue of non-malicious insider threats, which are on the rise in businesses, is the main topic of the study article. These risks are brought on by well-intentioned workers who inadvertently hurt others by their behaviour or a failure to comprehend cybersecurity rules and procedures. Instead of focusing exclusively on technological fixes, the article investigates how these vulnerabilities might be reduced from a human cybersecurity viewpoint. It talks about the value of training and educating employees as well as the need for simple, clear rules and processes that are consistently communicated and followed. The study also looks at how organisational culture affects how non-malicious insider threats are handled, emphasizing the need for a culture of security that motivates staff to put cybersecurity first.*

***Keywords -*** *Cyber Security, Vulnerabilities, Organisational Culture, Human-Centred Threat, Non-Malicious Threat.*

## 1. Introduction

Today's organisations must deal with various internal and external security concerns. The danger from inside, especially from benevolent insiders, is sometimes overlooked as threats from the outside, such as malware, phishing, and hacking, get a lot of attention. Insider threats that are not malevolent are unintended activities that staff members or other insiders perform that might jeopardise a company's security. These actions might include anything from accidentally exposing personal information to falling for a social engineering ruse. Regardless of whether insiders are malevolent, the damage they may do is still quite dangerous (Afzaliseresht et al., 2020). So, it is crucial to look at possibilities for lowering this type of hazard from the standpoint of human cybersecurity.

This paper explores the problem of insider threats in organisations that are not hostile and provides mitigating recommendations. The research focuses on non-technical safeguards that organisations might use to reduce insider threats. Some solutions include strengthening training programmes, implementing guidelines, and creating a friendly security culture (Afzaliseresht et al., 2020). The article is organized as follows: it begins with introducing insider threats and explaining what they are, as well as what they can accomplish. The characteristics of non-harmful insider threats are then discussed. Finally, it examines several mitigating strategies, including employee education and training, guidelines, and a supportive security culture. From the standpoint of human cyber security, the article concludes with recommendations for organisations on how to decrease insider risks that are not malevolent (Afzaliseresht et al., 2020).

### *1.1. Aim and objectives*

*1.1.1. Aim*

The aim of this essay is to discuss the growing problem of non-malicious insider threat in organizations and to explore how this type of human-centered threat can be mitigated from a human cybersecurity perspective, using non-technical approaches.

*1.1.2. Objectives*

1. To define what a non-malicious insider threat is and the various types of non-malicious insider threats.
2. To examine the factors that contribute to non-malicious insider threats, including organizational culture, employee motivation, and human error.
3. To identify the consequences of non-malicious insider threats for organizations, including financial loss, reputational damage, and regulatory non-compliance.

## 2. Literature Review

### *2.1. Employee Awareness and Training*

Giving staff education and training on cybersecurity best practices is one of the most efficient methods to reduce non-

malicious insider risks. With the use of this strategy, staff members are better able to spot possible threats, including phishing emails, social engineering, and weak passwords, as well as the value of safeguarding sensitive data. Organizations may greatly lower the danger of non-malicious insider threats by regularly offering training and reiterating these concepts. Non-malicious insider threats are unintended behaviours or omissions by staff members or other insiders that jeopardise the confidentiality of sensitive data held by an organization (Bevan et al., 2016). These may be errors like unintentionally transmitting private information to the incorrect person, misconfiguring security parameters, or falling for a phishing scam. Organizations must regularly teach their staff on cybersecurity awareness in order to reduce the potential of benign insider attacks. Best practices for protecting sensitive data should be covered throughout this training, including using strong passwords, avoiding public Wi-Fi, and not disclosing login information to other parties (Bevan et al., 2016).

Employees should also get training on possible dangers like phishing emails and social engineering ploys. They should be aware of the organization's rules and processes for managing security problems and be able to recognise and report any suspicious emails, links, or attachments. Making cybersecurity training a regular component of the onboarding process for new employees is crucial, as is offering ongoing instruction and reminders (Chandler, 2013a). To emphasize the value of maintaining excellent security measures, this may include simulating phishing attempts or other exercises.

### *2.2. Implementing Access Controls*

Implementing access controls that restrict employee access to certain data is another technique to counteract non-malicious insider risks. Limiting access based on job duties, adopting two-factor authentication, and keeping an eye on access logs for odd behaviour are all examples of access restrictions. This strategy lowers the possibility of data breaches brought on by non-malicious employees and helps to avoid inadvertent or unauthorized access to critical information. Access restrictions are a crucial part of any organization's successful security strategy (Chandler, 2013a). Companies may lessen the danger of non-malicious insider threats by restricting the quantity of data that workers have access to. These hazards might result from unintentional or illegal access. By limiting access to sensitive information based on a user's job, responsibilities, and clearance level, access controls function to make sure that only those who need access to a particular piece of information can get it (Chandler, 2013a).

Assigning certain rights based on an employee's job duties is one efficient technique to create access restrictions. For instance, a worker in the finance division could need access to financial information but not consumer information. An individual working in customer service, however, could need access to client information but not financial information (Chandler, 2013b). Companies may make sure that workers only have access to the data they need to carry out their job duties by establishing permissions based on these specifications. Adding two-factor authentication is a further technique to improve access control (2FA). In order to access sensitive data using this method, companies must give two means of authentication, such as a password and a security token or a fingerprint (Chandler, 2013b). Even if they have stolen a password or other credentials, it will be more difficult for unauthorized persons to access the data as a result of the additional layer of protection.

### *2.3. Developing a Strong Security Culture*

Non-malicious insider risks may be reduced in a business with a strong security culture. To do this, a culture that prioritizes security and encourages staff to report any suspicious behaviour must be established. By immersing staff in security activities, fostering a secure reporting environment, and rewarding security-conscious conduct, organisations may accomplish this. Organizations may lessen the possibility of benign insider threats and improve security by building a strong security culture (Davey and Wootton, 2017). In order to create a strong security culture inside a business, technological controls and security policies must be put in place, but it is also crucial to make sure that staff members recognise the significance of security. It entails fostering a culture in which security is everyone's responsibility rather than the exclusive purview of the IT division. Non-malicious insider threats, which often come about unintentionally and as a result of ignorance or neglect, might be lessened with the aid of such a culture (Davey and Wootton, 2017).

Organizations should include workers in security activities to create a strong security culture. The newest security dangers should be made aware to employees, who should also get regular security training. Individuals need to be encouraged to come forward with any security-related information without worrying about repercussions. It is essential to provide a secure reporting environment to motivate staff to speak up when they see anything unusual (Gill and Thomson, 2014). This entails designating a team or individual to whom staff members may report, as well as making sure that the reporting procedure is quick and private (Grech and Lutzhoft, 2016).

### *2.4. Implementing Clear Policies and Procedures*

Non-malicious insider risks may be reduced with the use of clear rules and procedures. Organizations should create and implement rules and procedures that specify authorised uses of data and information systems as well as the penalties for doing so. This strategy lowers the possibility of unintentional security breaches by ensuring that staff are aware of their duties. Insider threats that are not malicious may pose a serious danger to an organization's cybersecurity (Grech and Lutzhoft, 2016). These dangers may come from staff members

who accidentally jeopardise sensitive data or systems because of ignorance or carelessness. However, by creating and implementing clear rules and processes that define what constitutes authorised use of data and information technologies, businesses may reduce this risk (Ki-Aries and Faily, 2017).

These regulations must be thorough and cover all facets of the organization's data and information systems. These should specify what each employee's duties are, as well as what conduct is allowed while utilising the company's IT resources (Ki-Aries and Faily, 2017). This covers policies for managing passwords, using the internet, email, remote access, and social media. Policies and procedures should explicitly outline the repercussions for breaking these rules in addition to defining authorised usage. Discipline may range from warnings to complete termination of employment. Employees need to be aware of the repercussions of their actions and that they are in charge of safeguarding sensitive data held by the company (Ki-Aries and Faily, 2017).

### *2.5. Establishing Effective Communication*

In order to reduce insider risks that are not intentional, effective communication is essential. Companies should have open lines of communication for staff to use when reporting security-related occurrences or issues. This entails offering a safe method of reporting an occurrence, such as a hotline or email address, and making sure that staff members are aware of the procedure. Organizations can react promptly to security problems and lessen the impact of benign internal threats by setting up efficient communication channels (Reece and Stahl, 2015). Good communication is crucial for reducing non-malicious insider threats, which are instances that happen accidentally as a result of carelessness or ignorance, as opposed to deliberate sabotage. Serious repercussions from such situations may include the loss of confidential information, financial loss, damage to one's reputation, and legal culpability (Reece and Stahl, 2015).

Organizations must provide open lines of communication that allow staff to quickly report security-related occurrences or concerns in order to avoid similar incidents. In order to do this, employers must provide staff with a safe reporting method that guarantees confidentiality and anonymity, such as a hotline, email address, or web-based form. Organizations must also make sure that workers know how to report events and value the need to do so (Renaud and Flowerday, 2017). This may be accomplished via ongoing training and awareness programmes that emphasise the dangers and repercussions of insider threats as well as the need to report any suspicious activity or occurrences without delay.

## 3. Methodology

The non-malicious insider threat refers to the risk posed by trusted employees or contractors who, intentionally or unintentionally, cause harm to an organization's information or assets. This type of threat is growing, and it can be difficult to detect and prevent because the insider has legitimate access to the organization's systems and data (Renaud and Flowerday, 2017).

To mitigate the risk of non-malicious insider threats from a human cybersecurity perspective, organizations can take several steps:

### *3.1. Employee Education and Awareness*

Workers need to be informed about the dangers posed by insider threats and how they may help to lessen the risk. Training on information security best practices, such as avoiding phishing scams and safe data handling procedures, may fall under this category.

Organizations should provide specialist training on insider threats in addition to basic training on information security best practices (Scott, 2017). Employees could benefit most from this training by learning about the various insider dangers, such as malevolent and unintentional insiders. Workers should also be made aware of the many methods in which these dangers could materialize, such as via the theft of private data, system sabotage, or illegal access to data (Scott, 2017).

The warning signals of possible insider threats, including changes in behaviour or access patterns, should be included in insider threat training as well. The firm should have clear reporting routes and standards in place to guarantee that these complaints are handled correctly. Workers should be encouraged to report any suspicious behaviour to their managers or IT security specialists (Volkamer et al., 2015).

### *3.2. Establish Clear Policies and Procedures*

Employees should be asked to sign off on the organization's transparent rules and processes for data access and management. The rules should also specify the behaviours that are prohibited as well as the penalties for breaking them. For an organization to ensure the security and privacy of sensitive information, it is crucial to establish clear rules and processes for data access and management (Daniel Ani, He, and Tiwari, 2016). These rules need to outline the proper methods for gathering, processing, storing, transmitting, and discarding data. They should also specify the obligations of various parties, including management, workers, and IT personnel, in maintaining data security.

Employees should be forced to sign off on policies and procedures to show that they understand them. This would show that they are aware of and agree with the regulations regulating data access and management (Daniel Ani, He, and Tiwari, 2016). Also, to keep staff members informed of any policy changes or emerging dangers to data security, frequent training and awareness workshops should be made available to them.

### *3.3. Regular Monitoring*

Potential insider threats may be found early on with regular employee behaviour monitoring. This might include keeping an eye on how employees access data, observing system activity, and looking for unusual patterns in network traffic. A proactive approach to identifying and addressing possible insider threats in the workplace may be achieved by routinely monitoring employee behaviour (De Waard et al., 2016). Organizations can swiftly identify any illegal access or unusual conduct, such as efforts to edit or delete crucial files, by tracking employee access to important data and watching system activity.

Analyzing network data for anomalies may also assist in identifying odd behaviours or trends that can point to an insider threat (De Waard et al., 2016). An employee could be up to something sinister if they suddenly start accessing significant volumes of data outside of their regular working hours, for instance.

Nevertheless, it is crucial to remember that although keeping an eye on employee behaviour may be useful in eliminating insider threats, it must be done in a manner that respects employee privacy and complies with legal and ethical requirements. Companies should develop clear rules and processes for employee monitoring and make sure that workers are informed of the actions being monitored and their purposes (Medeiros et al., 2016).

### *3.4. Implement Data Access Controls*

To restrict the quantity of data that workers have access to, organisations might install data access rules. This may lessen the potential harm brought on by an insider danger that isn't intentional. A key component of safeguarding the security of sensitive data inside an organization is the implementation of data access controls (Medeiros et al., 2016). Organizations may lower the risk of data breaches, data leaks, and other cybersecurity issues by restricting the amount of data that workers have access to.

Moreover, data access policies may shield the company from unintentional damage from non-malicious insider risks. For instance, a worker can unintentionally delete or edit information that they should not have had access to in the first place, which might have major repercussions for the company (Chandler, 2012).

### *3.5. Foster a Positive Company Culture*

The danger of insider threats may be decreased with a strong corporate culture. Companies should establish a working atmosphere that promotes open communication and encourages staff to report any questionable activity. Beyond lowering the possibility of insider threats, fostering a healthy workplace culture may offer a number of advantages. Employees are more likely to be productive, motivated, and dedicated to the organization's objectives when they feel valued and involved (Chandler, 2012). A healthy culture may also increase employee retention rates and attract top talent, saving the business time and money on hiring and training.

Generally, a mix of technological and non-technical measures is needed to mitigate non-malicious insider risks. Organizations may lower the risk of insider threats and safeguard their data and assets by putting these measures in place.

## 4. Discussion and Analysis

Non-malicious insider threat refers to the unintentional or accidental actions of employees, contractors, or other trusted individuals that may compromise the security of an organization. This type of threat is becoming more prevalent, and it can be challenging to mitigate as it often involves human behavior rather than technical vulnerabilities. However, there are several ways in which organizations can address this issue from a human cybersecurity perspective (Fairburn et al., 2021).

### *4.1. Education and Awareness*

Employee education on the value of cybersecurity and the dangers of their conduct is one of the best strategies to reduce non-malicious insider threats. Regular training sessions, seminars, and workshops on subjects like phishing, social engineering, and password management might be a part of this. Organizations may lower the likelihood of unintended insider events by increasing awareness and arming staff with the information they need to recognise and report possible risks. Incidents involving unintentional damage to a company's data, systems, or network are referred to as non-malicious insider threats (Fairburn et al., 2021). These mishaps may be brought on by a failure to comprehend or be aware of the organization's cybersecurity rules, processes, and best practices. Moreover, they may be the consequence of human mistakes, such as opening a malicious file or link in an email or falling for a phishing hoax.

Organizations should provide all staff with priority cybersecurity awareness training to lower the danger of non-malicious insider attacks. A wide variety of issues, including spotting and reporting suspicious activity, using strong passwords and multi-factor authentication, and developing safe surfing practices, should be covered in the thorough training (Quagliarini et al., 2021). It is crucial to remember that cybersecurity training should be a continuous activity rather than a one-time event. To emphasize the value of cybersecurity and keep staff members informed of the most recent risks and best practices, regular training sessions, seminars, and workshops should be held. A security awareness programme that exposes workers to mock phishing attempts and other security checks should be implemented by organisations. Employees may practise seeing and reporting suspicious behaviour in a secure setting as a result (Quagliarini et al., 2021).

### *4.2. Clear Policies and Procedures*

Companies should have clear rules and processes in place that regulate employee conduct with regard to cybersecurity. All staff members should be made aware of these rules in a straightforward manner, and they should be routinely updated to reflect changes in the threat environment. Organizations may lessen the chance that staff members will unintentionally compromise the organization's security by outlining clear rules for appropriate conduct (Codreanu, 2021). Organizations need to take proactive measures to protect themselves against the sophisticated and pervasive cyber dangers that are present in today's digital world. Implementing clear rules and processes that control employee behaviour with regard to cybersecurity is one of the most efficient methods to do this. These guidelines should be thorough and include every area of cybersecurity, including password management, email use, social media policy, remote working guidelines, and more. They should also specify the repercussions for breaking these rules, which may include disciplinary action, loss of employment, and in some circumstances even legal repercussions (Codreanu, 2021). All workers should be made aware of these rules in a clear and consistent manner to guarantee their effectiveness. Moreover, staff should get frequent training to keep them informed about the most recent dangers and the best methods for defending against them. In order for the business to respond quickly to minimize any harm, this training should also address how to recognise and report possible security problems (Renaud and Coles-Kemp, 2022).

### *4.3. Role-Based Access Controls*

Role-Based Access Controls (RBAC) are a powerful tool for mitigating insider threats. RBAC involves assigning access permissions to employees based on their role in the organization, and it ensures that employees can only access the information and systems that they need to perform their job functions. By limiting access to sensitive information and systems, organizations can reduce the risk of non-malicious insider incidents. Role-Based Access Control (RBAC) is a widely used access control model that grants or denies access rights to resources based on the roles and responsibilities of the users within an organization (Renaud and Coles-Kemp, 2022). The RBAC approach ensures that employees have only the permissions necessary to perform their job duties, thereby reducing the risk of accidental or deliberate misuse of sensitive data and systems.

In an RBAC system, access is granted based on an employee's job function and is typically implemented through a hierarchical structure of roles, permissions, and access control policies. Each employee is assigned a specific role within the organization, and that role is associated with a set of access permissions that correspond to the employee's responsibilities. This approach provides a clear and defined system of accountability for access to sensitive information and systems, and it helps to prevent unauthorized access by limiting the number of employees who have access to sensitive data (Hoem, Veitch, and Vasstein, 2022). By limiting access to sensitive information and systems, RBAC helps to mitigate the risk of non-malicious insider incidents, such as accidental data leaks or unintentional damage to systems. Additionally, RBAC can also be used to prevent malicious insider threats, such as employees intentionally stealing sensitive data or sabotaging systems. RBAC provides a mechanism for detecting and preventing unauthorized access by monitoring user activity and enforcing access control policies (Hoem, Veitch, and Vasstein, 2022).

### *4.4. Monitoring and Detection*

Companies should put in place monitoring and detection tools that can quickly spot insider risks. This may include watching for odd patterns of activity, access to private data, or efforts to get around security measures in the course of employee behaviour. Organizations may take measures to stop events from escalating by identifying potential issues early. In order to detect possible threats in real time and reduce the danger that insider threats represent to an organization's security, monitoring and detection systems must be put in place (Cherrington et al., 2020). Organizations may use these technologies to monitor employee behaviour and look for any odd patterns of conduct that could point to an insider threat. For instance, monitoring systems may assist in identifying when a worker accesses private data when it is not necessary for their job or does so at odd hours. Security personnel may be notified of suspected data breaches or thefts as a result.

Monitoring tools may also be used to spot staff efforts to go around security measures by turning off security features or installing illegal software. These behaviours might be a sign of malevolent intent and can aid security teams in developing preventative measures (Cherrington et al., 2020). Organizations may avoid these occurrences from growing and inflicting serious damage to the business through early identification of insider threats. Security teams may investigate and take the necessary action to reduce the risks if they are discovered. These actions might include removing access credentials, adding more security measures, or even dismissing the individual.

### *4.5. Culture of Security*

Lastly, businesses should foster a culture of security that highlights the significance of cybersecurity and motivates staff to give it top priority in their everyday tasks (Zhou, 2021). This might include praising and rewarding staff members who use sound cybersecurity procedures, giving frequent performance reviews, and fostering open dialogue about possible dangers. Organizations may guarantee that cybersecurity is a high concern for all workers and that everyone is cooperating to lower the risk of insider threats by building a culture of security. In order to defend against cyber attacks, an organization's culture of security is essential. Organizations must foster a culture where workers value

cybersecurity and are encouraged to take the required safeguards (Zhou, 2021). Relying exclusively on technological solutions like firewalls and antivirus software is not sufficient.

Recognizing and rewarding staff members who implement sound cybersecurity procedures is one method to foster a culture of security. This can include thanking staff members in public who disclose possible security lapses or who constantly adhere to security guidelines. Employees are more likely to continue to be alert and prioritize security when they feel that their efforts to safeguard the company are respected and appreciated (Murphy, Carew, and Stapleton, 2022). Regular performance feedback is a crucial component of a security culture. Companies should provide staff with the opportunity to practise and evaluate their abilities while also providing continuing training and instruction on cybersecurity best practices. Frequent evaluations may also aid in identifying areas that could need more training or assistance (Murphy, Carew, and Stapleton, 2022).

Non-malicious insider threats are an increasing issue for enterprises, but from the standpoint of human cybersecurity, there are a number of strategies to counter this sort of danger. Organizations may lower the risk of unintended insider events and safeguard their sensitive data and systems by training staff, creating clear rules and procedures, utilising role-based access restrictions, monitoring and detection, and building a culture of security (Murphy, Carew, and Stapleton, 2022).

## 5. Conclusion

In conclusion, non-malicious insider threats are a significant and growing problem for organizations. These threats can arise from unintentional mistakes, carelessness, or simply a lack of knowledge. The cost of these threats to organizations can be high, both financially and in terms of reputational damage. Mitigating non-malicious insider threats requires a multifaceted approach that addresses the human factor of cybersecurity.

This includes education and awareness training for employees, implementing policies and procedures that promote good cyber hygiene, and creating a culture of security within the organization. Some specific strategies that can be used to mitigate non-malicious insider threats include conducting regular security assessments, implementing access controls and monitoring systems, and using technologies such as encryption and data loss prevention tools.

## References


[1] Neda Afzaliseresht et al., "From Logs to Stories: Human-Centred Data Mining for Cyber Threat Intelligence," *IEEE Access*, vol. 8, pp.19089-19099, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Yoshinobu Akimoto et al., "Approach Function Study for Concierge-Type Robot by Model-based Development with User Model for Human-Centred Design," *ROBOMECH Journal*, vol. 3 no. 1, pp. 1-13, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[3] Nigel Bevan et al., "New ISO Standards for Usability, Usability Reports and Usability Measures," *Human-Computer Interaction. Theory, Design, Development and Practice: 18th International Conference, HCI International 2016*, Toronto, ON, Canada, vol. 9731, pp. 268-278, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[4] David Chandler, "Resilience and Human Security: The Post-Interventionist Paradigm," *Security Dialogue*, vol. 43, no. 3, pp. 213-229, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[5] David Chandler, "Human-Centred' Development? Rethinking 'Freedom' and 'Agency' in Discourses of International Development," *Millennium: Journal of International Studies*, vol. 42, no.1, pp. 3-23, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[6] David Chandler, *Freedom vs Necessity in International Relations: Human-Centred Approaches to Security and Development*, 1st ed., Bloomsbury Publishing, 2023. [Google Scholar] [Publisher Link]

[7] Marianne Cherrington et al., "Features of Human-Centred Algorithm Design," *2020 30th International Telecommunication Networks and Applications Conference (ITNAC)*, Melbourne, VIC, Australia, pp. 1-6, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[8] Claudiu Mihai Codreanu, "Exploring the need for Human-Centred Cybersecurity, The WannaCry Cyberattack," *Romanian Journal of Society and Politics*, vol. 15, no. 2, pp. 1-21, 2021. [Google Scholar] [Publisher Link]

[9] Uchenna P. Daniel Ani, Hongmei Mary He, and Ashutosh Tiwari, "Human Capability Evaluation Approach for Cyber Security in Critical Industrial Infrastructure," *Advances in Intelligent Systems and Computing*, pp. 169-182, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[10] Caroline L. Davey, and Andrew B. Wootton, *Design Against Crime: A Human-Centred Approach to Designing for Safety and Security*, 1st ed., Taylor and Francis, 2017. [Google Scholar] [Publisher Link]

[11] Max Bernhagen, Patrick Roßner, and Angelika C. Bullinger, "Human-Centred Development of Automatically Accommodating Contact Lenses," *Chemnitz University of Technology*, Germany, 2016. [Google Scholar]

[12] Allan Dwyer, Measuring Human Security: The Why and the How, 2012. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2018964

[13] Nicola Fairburn et al., "Beyond Murphy's Law: Applying Wider Human Factors Behavioural Science Approaches in Cyber-Security Resilience," *HCI for Cybersecurity, Privacy and Trust: Third International Conference, HCI-CPT 2021, Held as Part of the 23rd HCI International Conference, HCII*, Springer, Cham, vol. 12788, pp. 123-138, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] Scherto Gill, and Garrett Thomson, *Rethinking Secondary Education: A Human-Centred Approach*, 1st ed., Routledge Taylor and Francis Group, 2014. [Google Scholar] [Publisher Link]

[15] Michelle Rita Grech, and Margareta Lutzhoft, "Challenges and Opportunities in User Centric Shipping: Developing A Human Centred Design Approach for Navigation Systems," *Proceedings of the 28th Australian Conference on Computer-Human Interaction - OzCHI '16*, Association for Computing Machinery, New York, NY, United States, pp. 96-104, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[16] Asa S. Hoem, Erik Veitch, and Kjetil Vasstein, "Human-Centred Risk Assessment for a Land-based Control Interface for an Autonomous Vessel," *WMU Journal of Maritime Affairs*, vol. 21, no. 2, pp. 179-211, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] Duncan Ki-Aries, and Shamal Faily, "Persona-Centred Information Security Awareness," *Computers and Security*, vol. 70, pp. 663-674, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[18] Kitty Kioskli et al., "The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity - Hygiene in Healthcare 4.0," *Applied Sciences*, vol. 13, no. 6, pp. 1-16, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[19] Derek McAuley et al., "Human-Centred Home Network Security," *arXiv preprint*, pp. 1-18, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[20] Andrew S. Medeiros et al., "Water Security for Northern Peoples: Review of Threats to Arctic Freshwater Systems in Nunavut, Canada," *Regional Environmental Change*, vol. 17, no. 3, pp. 635-647, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[21] António Moniz, "*Robots and Humans as Co-Workers the Human - Centred Perspective of Work with Autonomous Systems*," IET/CESNOVA, pp. 1-21, 2013. [Google Scholar] [Publisher Link]

[22] Cian Murphy, Peter J. Carew, and Larry Stapleton, "Ethical Personalisation and Control Systems for Smart Human-Centred Industry 5.0 Applications," *IFAC-PapersOnLine*, vol. 55, no. 39, pp. 24-29, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[23] Pengiran Salleh Ab Rahaman, "*A Human-Centred Approach to National Identity Management Systems*," Doctoral Thesis, UCL, 2012. [Google Scholar] [Publisher Link]

[24] Enrico Quagliarini et al., "Risk Reduction Strategies Against Terrorist Acts in Urban Built Environments: Towards Sustainable and Human-Centred Challenges," *Sustainability*, vol. 13, no. 2, pp. 1-29, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[25] R.P. Reece, and B.C. Stahl, "The Professionalisation of Information Security: Perspectives of UK Practitioners," *Computers and Security*, vol. 48, pp. 182-195, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[26] Karen Renaud, and Lizzie Coles-Kemp, "Accessible and Inclusive Cyber Security: A Nuanced and Complex Challenge," *SN Computer Science*, vol. 3, no. 5, pp. 1-14, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[27] Karen Renaud, and Stephen Flowerday, "Contemplating Human-Centred Security and Privacy Research: Suggesting Future Directions," *Journal of Information Security and Applications*, vol. 34, pp. 76-81, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[28] JKL Scott, "Phobic Cartography: Human-Centred, Communicative Analysis of the Cyber-Threat Landscape," *Journal of Information Warfare*, vol. 16, no. 4, pp. 93-112, 2017. [Google Scholar] [Publisher Link]

[29] Melanie Volkamer et al., "Design and Field Evaluation of PassSec: Raising and Sustaining Web Surfer Risk Awareness," *Trust and Trustworthy Computing: 8th International Conference, TRUST 2015*, Heraklion, Greece, vol. 9229, pp.104-122, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[30] Jiayi Zhou, "The (Universal) Human and Beyond: Constituting Security Objects in Theory and Practice," *Critical Studies on Security*, vol. 10, no. 1, pp. 16-29, 2022. [CrossRef] [Google Scholar] [Publisher Link]