HUMAN ASPECTS TO FORENSICS

BISF 3105

ASSIGNMENT ONE

CAMPUS: MAIN

FULL TIME

PRESENTED TO GLADYS MANGE

Group Members.

1. Kevin Kiplagat – 20/03551
2. Gillian Sheila – 20/03688
3. Emmanuel Sigei – 20/03807

ASSIGNMENT ONE.

1. **Write short notes on the 7 aspects of human beings.**

People form their own worldviews and perspectives on life based on their personal experiences and external influences that directly affect them, which impacts their understanding of themselves, others, and the world. After significant research and study, Revel Miller has simplified this complicated concept into "The Life Wheel: 7 Aspects of Who You Are." (Miller, 2001) These seven aspects represent the key characteristics that define us and form the foundation of our nature. For Revel Miller, this perspective shaped how he observed and interacted with others in order to help them achieve their personal goals and improve their quality of life. These Seven aspects also lay a solid foundation for understanding the complexity of human identity and development. (Maslow, 1943).

The 7 Aspects

The 7 Aspects of human beings are the Spiritual aspect, the Emotional aspect, the Mental aspect, the Physical aspect, the Behavioral aspect, the Social aspect and the Self Aspect as explained below:

i). Spiritual aspect.

This aspect is concerned with our personal search for meaning and purpose in life. It encompasses our beliefs, values, and connection to a higher power or to our inner selves. It delves deeply into existential questions and the search for enlightenment assisting us in our quest for personal fulfillment.

ii). Emotional aspect.

The emotional aspect is concerned with our realm of feelings and emotions. It involves important personal matters such as self-awareness and our ability to understand and manage our emotions.

iii). Mental aspect.

This aspect encompasses our thinking, reasoning, problem-solving, acquisition of knowledge, critical thinking skills, and intellectual development.

iv). Physical aspect.

This aspect focuses on our bodies and their well-being and encompasses nutrition, exercise, and overall health. This aspect also directly impacts the other aspects, since a healthy body can positively influence emotional, mental, and social well-being.

v). Behavioral aspect.

The behavioral aspect relates to our actions, habits, and lifestyle choices and It reflects the outward expression of our thoughts, emotions, and beliefs.

vi). Social aspect.

The social aspect emphasizes our interpersonal relationships and our role within various social contexts such as family, friends, our communities, and our professional networks.

vii). **Self-Aspect.**

This aspect is sometimes considered the "Main" aspect of our identity and includes self-esteem, self-perception, and self-acceptance. It acts as a reflection of how individuals perceive and relate to themselves.

2. **How can human factors affect the security and forensics of information systems? Describe a few instances.**

Human factors play an important role in information system security and forensics. Here are examples of how human factors can affect safety and forensics (Human Factors Research Center at the University of California, 2018)

i. **Social engineering.**

Human factors such as trust, gullibility, and willingness to help others can make individuals vulnerable to social engineering attacks. Attackers can impersonate someone in a position of authority, such as a senior executive, to manipulate employees into revealing sensitive information, such as passwords or access credentials. access.

ii. **Forensics investigations.**

During forensic investigations, human factors can affect the preservation and integrity of digital evidence. Mishandling or improper storage of digital devices, failure to document the chain of custody, or lack of knowledge of the legal and procedural aspects of forensics can compromise the results investigate.

iii. **Insider treats.**

Employees or individuals with privileged access to information systems may intentionally or unintentionally compromise security. Human factors, such as dissatisfaction, financial stress or lack of appropriate training, can contribute to insider threats. Surveillance and early detection are crucial in such cases.

iv. **Password security.**

Human factors such as password selection and management can have a significant impact. Weak passwords, password sharing, and password writing can lead to unauthorized access

v. **Biometric authentication.**

Biometric identification methods that rely on human characteristics like fingerprints and facial recognition might be subject to impersonation. This therefore means that for security to be assured, the limits of these technologies should be well understood.

vi. **Phishing attacks.**

People's susceptibility to phishing emails and text messages is a good example. Users may click on malicious links or download infected attachments due to social engineering tactics. Their lack of awareness and caution can compromise the security of information systems.

vii. **User compliance.**

User willingness to follow security policies and procedures is heavily influenced by human factors. If users find security measures too cumbersome or unfriendly, they may be tempted to bypass security controls, which can create vulnerabilities.

viii. **User error.**
Accidental data breaches often occur due to human error. This can include sending sensitive information to the wrong recipient, misconfiguring security settings, or accidentally deleting important data. Proper training and use of protective measures can minimize these risks.

3. **What are the primary obstacles that businesses face in protecting their information systems from threats from people? How can these problems be solved?**
The following are the most major challenges and problems businesses face when protecting their Information Systems from attacks by threat actors (IBM, 2023)
   i). Disgruntled employees can compromise the security of the information system from within thus making the business vulnerable. This can however happen unintentionally for employees with good standing as well. To mitigate this, strong access control measures can be implemented, and awareness training conducted in-house by the business.
   ii). Social engineering tactics such as Phishing emails, baiting and pretexting can be used to manipulate human psychology. This can be mitigated by running simulated phishing attempts and awareness training.
   iii). The rising Bring Your Own Device (BYOD) trend raises another complexity for businesses since employees can introduce infected devices into the business network knowingly or unknowingly. This can be resolved by conducting regular checks on the devices employees bring to ensure that there is no compromise.
   iv). Security regulations and industry best practices can be expensive and complex to implement which might pose a major challenge for startups and small businesses. To mitigate this, these businesses can use cost-effective security tools as a way to bridge this gap.
   v). The dynamic nature of the threat landscape poses a major challenge since there's seemingly always something new coming up. Businesses should learn how to adapt to this dynamic landscape and come up with comprehensive and robust incident response guidelines.
   vi). Another major challenge businesses face is the fact that their employees might not be aware of the threats they are exposed to and due to this, they might not be able to understand the implications of their actions or lack thereof while operating these information systems. This can also be resolved by conducting awareness training.

4. **Information systems are vulnerable to several threats. Explain the different common threats against contemporary Information systems.**

   i). **Insider Threats** – Employees involved directly with the operation of the information systems can inadvertently expose data held in the system or compromise the system's security. These employees can either have a motive, eg personal grievances with the business or it might be caused by negligence and lack of awareness.

   ii). **Denial of Service Attacks** – These are attacks in which the system is flooded with excessive amounts of spam traffic which in turn makes it inaccessible to the people who need to access the system thus disrupting operations.

   iii). **Social Engineering** – In Social Engineering, threat actors manipulate human emotions and psychology to gain access to the information or to convince an authorized individual to share sensitive information from the information system. Some of the techniques used include intimidation or masquerading.

   iv). **Malware Attacks** – Malware refers to any malicious software tools that are used by threat actors to infect computers and computer networks and thereafter steal data. These malicious software tools include (But are not limited to) Trojans, Ransomware and computer viruses. Threat actors use techniques such as infected emails and websites to plant these malware tools onto the computers of unsuspecting individuals.

   v). **Human Error** – This involves negligence and/or lack of awareness from users. It can range from leaving doors to server rooms open for example to leaving accounts logged in on publicly accessible computers. This therefore gives access to threat actors who can steal data.

   vi). **Physical intrusion** – This refers to instances where the threat actors forcibly gain access to buildings that house critical hardware and software infrastructure for running the information system.

   vii). **Physical Threats –** This includes instances where actual damage to hardware equipment is experienced. This can be caused by occurrences such as fires and natural disasters like floods.

   viii). **Man-in-the-Middle Attacks** – MitM attacks occur when threat actors intercept communication while it is still en route (eavesdropping), therefore gaining access to data that they can then change/alter before it reaches the intended recipient.

   ix). **Zero-Day Vulnerabilities –** Zero-day vulnerabilities are vulnerabilities in a software solution that go unnoticed by the software's developers. This presents an opportunity for threat actors to exploit and gain access to systems and thereafter pose a continuing challenge to the system's security.

5. **Explain the key technological trends that heighten ethical concerns.**
    i). **Artificial intelligence –** AI is increasingly making decisions that affect our lives, from job recruitment to healthcare diagnosis. The ethical concern is ensuring AI decisions are transparent, free from bias, and made in the best interests of individuals.

    ii). **Surveillance Technology –** With advanced surveillance tools, our every move can be tracked. While this can enhance security, it raises ethical issues around privacy and the potential for abuse of power.

    iii). **Deepfake Technology –** Deepfakes, which use AI to create highly convincing fake videos and audio, raise ethical issues related to misinformation, privacy invasion, and identity theft.

    iv). **Big Data –** The collecting and analysis of massive volumes of personal data with the aim of the development of data-driven services raises privacy concerns if the personal information is not responsibly used.

    v). **Gene Editing -** Genetic Engineering tools such as CRISPR-Cas9 gene editing tools allow us to make precise alterations to DNA structure. Although this technology has the ability to cure diseases, the ethical issues raised by it are the likelihood of unforeseen impacts such as the development of new diseases. (Isasi, 2017)

6. **Identify and describe six ethical principles.** (Holly Forester-Miller, 1996)
    i). **Justice –** This principle of Ethics encompasses everything to do with fairness and treating people equitably and advocates for the fair distribution of resources and burdens among individuals or among a group of people.

    ii). **Veracity –** Veracity refers to the act of being honest, open, transparent and trustworthy. For the world of Technology for example, this could mean being transparent with how algorithms used in software tools operate.

    iii). **Fidelity –** Fidelity refers to the act of being faithful and sticking to agreements. This ethical principle acts as a guide to the ensuring of confidentiality. In the Tech World, Fidelity can be related to the secure and confidential handling of data entrusted to us by users of our systems and platforms.

    iv). **Beneficence –** Beneficence refers to the performance of acts that seek to benefit others instead of bringing harm to them. In the tech world, beneficence could be demonstrated by for example implementing enough security features for applications which would in turn less expose the users to data breaches and attacks.

    v). **Non-Maleficence –** Non-maleficence involves only performing activities that would not cause harm to others. In the Tech landscape, Non-maleficence can be demonstrated by

actions such as responsibly handling user data thus not letting it land in the wrong hands where it could be used against the owners.

vi). **Autonomy –** Autonomy refers to letting people make their own choices and decisions by respecting people's independence. This can be demonstrated in the Tech Landscape by letting users for example decide what features and data on their phone your application can access through the use of the Permissions feature.

References

1. Holly Forester-Miller, T. D. (1996). *A Practitioner's Guide to Ethical Decision Making.* American Counseling Association.
2. Human Factors Research Center at the University of California, B. (2018). *Human Factors in Cybersecurity: Challenges and Solutions.* California: University of California, Berkeley.
3. IBM. (2023). *IBM Cost of a Data Breach Report 2023.* IBM.
4. Isasi, R. &. (2017). *Ethical and social issues in gene editing: Human germline editing and beyond.* Springer Nature.
5. Maslow, A. H. (1943). A theory of human motivation. *Psychological Review*, 370-396.
6. Miller, R. (2001). *The Life Wheel: 7 Aspects of Who You Are.* Career Quest, Inc.

ASSIGNMENT TWO.

QUESTION ONE:

How user behavior affects the efficacy of security mechanisms and best practices for enhancing this human behavior.

User Behavior greatly affects the efficacy of security measures implemented to protect systems either dictating success or failure. Below are some of the ways the behavior affects it:

1. When users create weak passwords or reuse passwords across different accounts, they undermine security measures since it gives the threat actor an easier time when trying to forcefully access these accounts.
2. Users can end up clicking on suspicious and malicious links which can end up undermining security measures by giving an opportunity to threat actors to implant malware and other such tools into the system.
3. Users can either intentionally or unintentionally disable security software such as Antivirus Tools or Firewalls thus compromising system security.
4. Users can carelessly handle sensitive data linked to the information system therefore providing a gateway for threat actors to access the system thus undermining the security measures implemented to protect the system.

Best Practices for enhancing this human behavior.

1. Businesses and organizations should invest in security and awareness training to build capacity within their teams.
2. There should be a standard and a benchmark set up for how strong and secure passwords used should be which would ensure no substandard passwords are being used.
3. Security audits should be conducted frequently and regularly to ensure adherence to security best practices implemented within the environment being used.
4. To prevent and deal with carelessness, irresponsibility and neglect, there should be consequences implemented for users who violate security best practices.

QUESTION TWO

How Social Engineering attacks undermine Information System Security and what actions businesses can take to stop these attacks.

Social Engineering attacks are attacks in which the threat actor uses manipulation techniques to have individuals share critical or sensitive information or to perform actions that directly compromise the security of an information system.

How Social Engineering Attacks Undermine Information System Security.

1. They can be used to gain Unauthorized Access to systems and the data held within the system through the use of deceptive tools and techniques such as manipulation.
2. Phishing attacks/attempts can be used to install malware onto computers used for the information system thus compromising it.
3. Social Engineering attacks such as baiting can lead to the implanting of malware-infected drives or disks in computers used to run the information system thus compromising the Security of the said Information System.
4. Pretexting can be used to create false scenarios in which unsuspecting users can be led to share their login credentials with threat actors. This compromises the security of the system.

Actions that can be taken to stop these attacks.

1. Employees can be educated on the existence of such threats and how to handle suspicious and/or unexpected communications that they receive from outside the business.

2. Robust security policies should be implemented regarding access to sensitive information or the information system in its totality.
3. Strong access control measures should be taken to limit access to sensitive information to only those who need it thus protecting the information system from unauthorized use.
4. Security needs to be beefed up by layering it e.g., through the use of Multi-Factor Authentication which can prevent access even if the threat actor has correct login credentials.

ASSIGNMENT THREE.

QUESTION ONE.

How can businesses strike a balance between user liberty, privacy, and security needs? What moral factors need to be taken into account in this situation?

Businesses can strike liberty between user liberty, privacy, and security needs in the following ways.

1. Having clear policies and regulations that govern how data is collected, which data is collected, how it will be used by the business, and how it will affect the customer.
2. Ensuring that before collecting any information from their consumers, they first have consent from them and clearly state why they are collecting the information. Consumers are at liberty to accept or refuse their data from being collected.
3. Having a data controller and a data processor will ensure that the data they collect will only be used for the purpose it was collected for.
4. Anonymizing and encrypting data collected from consumers to protect their consumer rights and needs.
5. Businesses should seek consent from consumers before sharing their data with a third- party so as not to infringe on user privacy, liberty, and security needs.
6. Collecting only data that is necessary and that is going to be used for the intended purpose and should not contain any irrelevant or excessive data that when used could violate the users' privacy.

What moral factors can be taken into account in this situation?

1. **Honesty and truthfulness**- Businesses should always be truthful in their data practices i.e., always inform the customer why the data is collected and what it will be used for beforehand.
2. **Accountability and responsibility**- Businesses should be accountable and responsible for customers' data that they collect. In case the customers' privacy and data are breached, they should take full responsibility for the damage it will cause.
3. **Respect for consent and autonomy** – customers should only provide data to organizations and businesses at their discretion. Businesses should be able to respect their decision about their data.
4. **Equality and fairness** – to strike a balance between user liberty, privacy, and security needs, businesses need to treat all customers equally and not based on the data to be collected from them.
5. **Transparency**- before consumers give out their data to businesses it is morally right to inform them of why, how, where, and when the data that is being collected is going to be used.
6. **Ownership of data**- businesses should acknowledge and respect the consumers as owners of the data they have collected and used.
7. **Data protection** – the business should be responsible and protect the data of the consumers that they have collected from any breaches to protect the consumers' privacy and be in compliance with the Data Protection Act of Kenya.
8. **Education**- consumers should be educated by the businesses on the type of data that they want to collect information, how they will use it and the importance of consent before they can collect and use their information to promote their business.

QUESTION TWO

What are the most important legal and regulatory matters that businesses should take into account while adopting information systems?

1. **Intellectual property rights** – while obtaining a new information system, businesses should ensure that the intellectual rights of the programmers and designers are not infringed upon.
2. **Copyright laws**- businesses should ensure that the information systems are adopting are not connected to any copyright laws and must be solely owned by the third party vending it to them or be their own.
3. **Obtaining copyright protection**- this is to ensure that an information system designed solely for the business remains the intellectual property of the business and can't be used by any other business.
4. **Data Protection Act** – Businesses must ensure that they are registered with the office of the data commissioner and have a data controller and a data processor to govern how data collected is going to be processed and used.
5. **Consumer protection laws**- The information system should not interfere with the consumer /customers' rights to be heard, have a choice, and be well-informed about the service or goods they want to acquire.
6. **Accessibility laws** – these laws ensure that the information system to be acquired by a business is sensitive and considerate to the needs of people with disabilities for example use of large fonts or adjustable fonts and color schemes to be inclusive for visually impaired people.
7. **E-commerce laws** – businesses who are adopting information systems for use in conducting their businesses online should comply with policies and regulations governing consumer rights, and online contracts among others.
8. **Employee and labour laws**- information systems that contain employee data are subject to this law. Businesses should ensure that employee data is protected and used only for the purpose that it was collected for. Fair labour practices should also be given to all employees.
9. **Anti-trust and competition laws** –Businesses using information systems should ensure that the systems do not facilitate anticompetitive practices such as price fixing or unfair business practices.
10. **International data transfer laws** – if the business is to operate internationally, before adopting an information system then the business is to consider the regulations that are associated with the cross-border data transfer laws.
11. **Software licensing laws**- for a business to obtain a software license the information system in question should their original work and does not violate any copyright laws or infringe on the rights of the user.