Respond to this based on the bellow post

**What are your thoughts about insider issues with opening emails? What should be the policy about those who continually open obvious spam mail? Should governmental agencies be able to release employees from their duties? What does that policy look like?**

How do we optimize/derive identity management and authentication procedures while balancing requirements for privacy including anonymity on the digital infrastructure?

Identity Management and Authentication Procedures

Identity management entails the authentication and identification of units which include hardware devices, people, software applications and distributed sensors. These entities can lead to the access of important information and solutions to counter any illegal access to the systems. I agree with this response to some extend because currently, there is a rise in interdependent systems thus identity management becomes an aspect to consider. The process involves identity establishment, oversight, accountability, credentials management, conflict resolution and the enforcement of important policies. Identity management is a broad sector which carries important and relevant information which is not limited to individuals identity numbers, identity cards, and biometric signatures. The future will require secure, understandable and flexible approaches because advancement in technology will be effective.

For identity management systems to be socially acceptable, it must allow the privacy of important information of an individual. When a person presents their private information to a particular site, the site should not learn any extra information apart from that which is required. A common problem facing people in the current world is cybercrime where criminals generate passwords by the use of different software hence accessing personal sites. This could be as a result of people using similar passwords to access different websites. Financial institutions have also been under the threat of impersonation leading to great losses (Hathaway, 2009). When the information needed is presented to a site, it becomes beneficial to everyone since privacy is well addressed.

Identity management systems will be successful after it has been able to solve the following key problems:

Authentication: This may involve the demonstration of identity in accordance with the schemes which are provided by various local authorities. For the many transactions carried out using credit-cards, verification involves checking that the purchaser has authority in spending that amount specified. The technological systems present make it easy for the card issuer assuring the dealer that the card is accredited for that particular volume claimed (Hathaway, 2009). The merchant gets assured that payment will take effect within a specified period.

Authorization: Authorization policies which can be easily maintained and audited are required for future responses.

Interaction in the cross-domain: Different branches in the same federal government can use a similar identity management system where authorization and authentication are left on the hands of local authorities (Hathaway, 2009).

Any solution offered to issues surrounding identity management should resist misuse and attack from attackers who have different motives. Insider attacks are common in this age hence institutions should effectively put measures to counter the threats. I agree with the authentication, cross-domain interactions and authorization effects which have been suggested to be important aspects in the identity management process. At the moment when the different organization have access to a common system in the government, use of the same password would make sure that information in these systems is secure and void of illegal human interactions

However, the response lacks an intensifying approach to how human factors, legal issues, the expectations of the society and usability can be addressed so that identity management can take place effectively. It will be a long term challenge in identifying the requirements which are required while different organizations are developing solutions managing to meet these requirements. In the near future, different enterprises will need management tools allowing them to operate successfully as their information is protected from external and internal threats.

Reference

Hathaway, M. E. (2009).

https://obamawhitehouse.archives.gov/files/documents/cyber/National%20Science%20Foundation%20-%20HathawayQuestions%20Mar%2031%202009.pdf