INFO 6010 - S2023 Assignment 2

Gihan Shamike Liyanage

1142109

CISSP Prep

29/07/2023

## Do government officials understand information security, and do they abide by the rules set out by their own organizations?

In today's world, information is increasingly digital and interconnected, and the safeguarding of sensitive government data has become a paramount concern. The proper understanding and implementation of information security protocols are vital for government officials who handle classified and confidential documents. However, recent incidents, such as the dismissal of Suella Braverman by the UK Prime Minister for violating ministerial rules, and the contentious case of Hillary Clinton's use of an unofficial email server in the United States, underscore the pressing need for a closer examination of how well government officials grasp information security principles and adhere to organizational regulations. Therefore, the significance of information security in the realm of governance and the implications of failures in adhering to established protocols is very important.

Suella Braverman, a UK government official, was dismissed by Prime Minister Liz Truss after violating ministerial rules. Braverman sent an official document from her personal email account to an MP, breaching information security protocols. Similarly, in the United States, Hillary Clinton faced controversy during her tenure as Secretary of State for using a private email server for official communications. The use of an unofficial server raised concerns about security, transparency, and compliance with government regulations. These incidents highlight the importance of understanding and adhering to information security measures for government officials, as lapses can have severe consequences for national security and public trust.

In my point of view, the root cause of both cases is similar and what went wrong in both cases was the mishandling of sensitive government information. Suella Braverman used her personal email for official communication, and Hillary Clinton employed an unofficial server, both violating information security protocols. Such actions risked the exposure of confidential data and raised concerns about transparency and national security. Media reports on such events are usually based on real incidents and facts rather than making something out of nothing. In both the Suella Braverman and Hillary Clinton cases, there were tangible actions that violated information security protocols and raised legitimate concerns about the handling of sensitive government information. Information security is a critical issue that requires attention from experts, governments, politicians, and their entourages. Mishandling of classified information can have severe consequences, such as data breaches, unauthorized access to sensitive data, compromised national security, and erosion of public trust. It is essential for information security experts to address these concerns and for governments and officials to take proactive measures to ensure proper handling of sensitive data and adherence to established protocols. Public scrutiny and media coverage can serve as catalysts for raising awareness and encouraging necessary reforms to strengthen information security practices.

To ensure that government representatives use appropriate means to protect their communications, a comprehensive approach is needed. Firstly, robust training and awareness programs should be implemented, emphasizing information security best practices and the consequences of mishandling data. Clear and well-defined policies and guidelines must be established, specifying approved channels for official communications, encryption protocols, and the handling of classified information.

Providing government representatives with secure communication tools, such as encrypted email systems and messaging platforms, is essential. Regular auditing and monitoring should be conducted to detect any security breaches or unauthorized usage. Accountability is crucial; mechanisms must be in place to hold representatives responsible for non-compliance with information security protocols, and appropriate consequences should be enforced. Promoting a culture of continuous education on information security matters encourages representatives to stay updated on the latest threats and best practices. Adequate IT support and resources are necessary to enable effective implementation of secure communication practices.

Collaborating with information security experts and organizations helps governments stay informed about evolving threats and seek advice on implementing robust security measures. By adopting this multi-faceted approach, governments can foster a culture of information security, ensuring that their representatives handle communications with the utmost care, safeguarding sensitive data, and upholding public trust in the process.

While some companies permit Bring Your Own Device (BYOD) policies to enhance flexibility and productivity, the context for government officials is distinct due to the sensitive nature of government data. Government communications often involve classified and confidential information, making it crucial to maintain stringent control over devices and data access. Allowing government officials to BYOD could increase the risk of data breaches, unauthorized access, and compromised national security. Therefore, most governments prioritize the use of secure, government-issued devices and communication tools to maintain a higher level of information security and protect sensitive data from potential vulnerabilities associated with personal devices.

Companies that allow BYOD (Bring Your Own Device), safeguarding company data on employees' personal smartphones becomes a top priority. To ensure the protection of sensitive information, several key measures can be implemented.

Initially, deploying Mobile Device Management (MDM) software is essential. MDM solutions allow IT administrators to remotely manage and secure employee devices. Features like data encryption, device tracking, remote wipe, and password policies can be enforced through MDM, bolstering data security. Mandatory security policies must be established and communicated to all employees. These policies should include requirements for strong passwords, biometric authentication, and automatic screen locking to prevent unauthorized access to company data.

Containerization technology can be employed to create separate encrypted containers for company data on employees' devices. This ensures that work-related information is isolated and protected, even if the personal device is compromised. Requiring employees to use a Virtual Private Network (VPN) when accessing company resources from their personal smartphones can add an extra layer of security to data transmission, safeguarding sensitive information from potential eavesdropping or data interception.

Regular software updates and patches are vital to maintaining device security. Encouraging employees to keep their devices up to date with the latest software releases and firmware updates helps mitigate potential vulnerabilities and ensures better overall security. Additionally, promoting data backup practices among employees is crucial. Encouraging them to back up their device data to secure cloud services or company servers helps prevent data loss in case of theft, damage, or accidental data deletion. Comprehensive employee education and training sessions are essential to raise awareness about BYOD policies and security best practices. This will ensure that employees understand the potential risks and know how to protect company data effectively.

Finally, the development of a well-defined incident response plan is crucial to handle security breaches, lost devices, or other security incidents promptly and efficiently. By diligently implementing these measures, companies can embrace BYOD to enhance productivity while maintaining robust data security to protect company information on employees' personal smartphones.

In conclusion, the significance of information security in governance cannot be understated, as seen in incidents involving Suella Braverman and the Hillary Clinton email controversy. A comprehensive approach is needed, including training, policies, secure tools, monitoring, and collaboration with experts. Government officials must prioritize data protection over BYOD, balancing productivity, and security. By emphasizing information security, governments uphold public trust, protect sensitive data, and ensure seamless operations in an interconnected world.

# References

Castle, M. L. (2022, Oct). *Liz Truss Fires Home Secretary Hours After Being Jeered in U.K. Parliament*. Retrieved from The New York Times: https://www.nytimes.com/2022/10/19/world/europe/liz-truss-uk-parliament.html

Graff, G. M. (2016, Sep). *What the FBI Files Reveal About Hillary Clinton’s Email Server*. Retrieved from Politico: https://www.politico.com/magazine/story/2016/09/hillary-clinton-emails-2016-server-state-department-fbi-214307/

Greenberg, A. (2015, Mar). *Why Clinton's Private Email Server Was Such a Security Fail*. Retrieved from Wired: https://www.wired.com/2015/03/clintons-email-server-vulnerable/

Rob Picheta, T. J. (2022). *Liz Truss plunged into deeper turmoil after Suella Braverman leaves as Britain’s Home Secretary*. Retrieved from CNN: https://www.cnn.com/2022/10/19/uk/suella-braverman-liz-truss-departure-gbr-intl/index.html

*Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton’s Use of a Personal E-Mail System*. (2016). Retrieved from FBI: https://www.fbi.gov/news/press-releases/statement-by-fbi-director-james-b-comey-on-the-investigation-of-secretary-hillary-clinton2019s-use-of-a-personal-e-mail-system

*Suella Braverman forced to resign as UK home secretary*. (2022, Oct 19). Retrieved from The Guardian: https://www.theguardian.com/politics/2022/oct/19/suella-braverman-departs-as-uk-home-secretary-liz-truss

*Suella Braverman resigns as home secretary*. (2022, Oct). Retrieved from Economist: https://www.economist.com/britain/2022/10/19/suella-braverman-resigns-as-home-secretary