Evaluation of Information Security within the e-Government Programme in Jordan: the connecting role of Citizens' Online Trust

Nadia Samara
PhD Management Candidate
Hull University Business School
N.K.Samara@2014.hull.ac.uk

Information Security in e-Government

Governments need to identify the main factors affecting e-government adoption in order to specify the strategies required to implement an e-government programme in a successful way. The Hashemite Kingdom of Jordan is one of the countries that has initiated an e-government programme to ensure the efficient delivery of services to the public and reduce the cost of delivering such services. Thus, the Jordanian government needs to identify barriers that may influence e-government adoption in order to specify an appropriate strategy.

Within the above context, the importance of information systems security remains critical. The risks of security attacks must be reduced to a minimum and citizens need to trust that the e-government programme will not expose them to risks. Thus, information security is an essential responsibility for any e-government programme, as such a programme has to address availability, confidentiality, integrity and accountability with regard to citizens' personal information. A high level of security will increase the level of trust and confidence among all stakeholders (whether citizens, businesses or government), and is the foundation of a successful e-government programme. In order to apply and select the required and appropriate security measures, the system assets must be identified, as well as analysing the perceived threats and vulnerabilities.

Accordingly, the aim of this study is to examine how Information Systems Security is evaluated and approached within the e-government programme in Jordan and provide an insight into the progress of various projects within it. The study examines the CIA information security triad (confidentiality, integrity, and availability) within the Jordanian e-government programme and aims to explore how information security is approached within the Jordanian e-government programme through the theoretical lens of the TFI (Technical, Formal and Informal) model in IS Security. The *technical* level concerns the hardware, software and networks; the *formal* one involves the policies, processes, procedures and all organisational-level security mechanisms. The *informal* level relates to individual-level

security mechanisms that become important at the level of organisation and include the role of factors such as the beliefs and attitudes of employees, security culture, values and awareness.

An important dimension of this research seeks to explore the way in which the government deals with citizens' personal information and how it communicates the security of its e-government programme in order to improve citizens' online trust and satisfaction; in turn, this may influence e-government programme adoption. A main concern for citizens remains information systems security and privacy within an e-government programme, as they fear that their information could be exploited or misused. Thus, this research focuses on *information security* and communicating security to establish *online trust* as key areas that influence the *adoption of e-government projects* in Jordan and tries to establish a link between the two. The core of the research will be conducted through a case-study of the e-government programme of the Ministry of Information and Communications Technology (MoICT) in Jordan. Semi-structured interviews will be conducted with officials and staff of e-government department. In addition, a survey of citizens will be conducted at government service-based organisations in order to explore online trust.

The TFI model for e-government security

Information security is an essential aspect to achieving business objectives through developing trust and minimising risk. For this reason, many researchers have explored the information security triad of confidentiality, integrity and availability (CIA) (Goluch et al. (2008); Peltier (2013)). In terms of information security architectures, Contreras (2013) proposes the zero trust model for cybersecurity. This model is based on dealing with all internal and external networks, on the assumption that all network traffic is untrustworthy. In practical terms, the principle of the zero trust model is that the user has to protect internal data from an insider attack, just as external data are protected in public networks (e.g., transactions within government agencies using an internal shared network or station, and transactions with other organisations via different networks using networked control systems). According to Ahlfeldt, Spagnoletti, and Sindre (2007), it is important to advance information security within administrative and organisational levels. The researchers also provide an extended model based on an IS perspective, involving technical, formal and informal levels, known as the TFI model. As these three parts interact continuously, the model proposes a comprehensive approach to the area of IS security. As mentioned above, the informal part includes fundamental norms, such as culture, beliefs, risks and awareness, which will operate and drive the design of the formal norms, for example, procedures, policies, standards, and so on. The technical part involves hardware, software and networks. This three-level view requires other issues to be addressed, such as trust and privacy, by means of new formal and informal mechanisms, such as identity management systems.

In the context of e-government, particularly in Jordan, Alomari, Sandhu, and Woods (2009) confirm that the government needs to address security in the design phase, in order to enhance public trust in e-government. Majdalawi, Almarabeh, Mohammad, and Quteshate (2015, p.219) state that "trust is a vitally

important component of e-government projects. Without trust, citizens who may already be cautious of using technology may avoid the use of online services that ask for detailed personal information". Therefore, these researchers suggest that the government should designate a senior official responsible for computer security; back up information regularly; train employees in computer security; continually assess systems to make sure that security precautions are being implemented; evaluate the performance of system managers in adhering to sound security practices; keep personal information collection to a minimum and not disclose personal information without express prior consent.

AbuAli and Almarabeh (2010) similarly assert that governments must handle the enormous amounts of personal information they hold carefully. Since governments collect data on their citizens through daily transactions, they have an obligation to protect the privacy of the personal information stored on their databases and make effective use of that information. Reffat (2003) also recommends that a government should educate and train government officials on the importance of privacy; design applications that integrate privacy protection; minimise the collection and retention of personal information; limit access to personally identifiable information; and not automatically allow employees to tap into databases of personally identifiable information. This is closely connected with data masking, which concerns the availability of data across organisational departments and employees. Access control and how access rights are granted to authorised users is a major issue in addressing information security within e-government systems. Furthermore, access control mechanisms must consider the internal transactions within an organisation, as well as the external transactions with other organisations and the public.

To conclude, the way in which governments deal with personal information and how secure their systems are will improve citizens' online trust and satisfaction, which will, in turn, influence e-government programme adoption. This places security *communication* at the core of the e-government programme (but in a controlled and limited way so that it does not expose the security of the e-government programme itself). In addition, information system security has a number of benefits, such as reducing corruption, because all transactions are monitored internally and externally using various security mechanisms and applications. It is also more likely that security attacks will be detected, prevented, or recovered, and perceived risks and threats will be analysed. Thus, this study will try to fill the gap in previous studies and focus on citizens' trust in and beliefs concerning e-government programmes from an information security perspective. As mentioned already, the latter part will be conducted through a survey of citizens.

References

AbuAli, A., & Almarabeh, T. (2010). A general framework for e-government: definition maturity challenges, opportunities, and success. *European Journal of Scientific Research, 39*(1), 29-42.

Ahlfeldt, R.-M., Spagnoletti, P., & Sindre, G. (2007). Improving the Information Security Model by using TFI. *In New Approaches for Security, Privacy and Trust in Complex Environments* (pp. 73-84): Springer US.

Alomari, M., Sandhu, K., & Woods, P. (2009). E-government adoption in the Hashemite Kingdom of Jordan: factors from social perspectives. *International Conference for Internet Technology and Secured Transactions, 2009. ICITST 2009*, 1-7.

Contreras, J. L. (2013). *Developing a Framework to Improve Critical Infrastructure Cybersecurity (Response to NIST Request for Information Docket No. 130208119-3119-01)*. Retrieved from SSRN 2248658:

Goluch, G., Ekelhart, A., Fenz, S., Jakoubi, S., Tjoa, S., & Mück, T. (2008). *Integration of an ontological information security concept in risk aware business process management* (1530-1605). Retrieved from Hawaii International Conference on System Sciences, Proceedings of the 41st Annual (pp. 377-377)

Majdalawi, Y. K., Almarabeh, T., Mohammad, H., & Quteshate, W. (2015). E-Government Strategy and Plans in Jordan. *Journal of Software Engineering and Applications, 8*(4), 211-223.

Peltier, T. R. (2013). *Information security fundamentals*: CRC Press.

Reffat, R. (2003). *Developing a successful e-government*. Retrieved from Proceedings of the Symposium on E-government: Opportunities and Challenge, Muscat Municipality, Oman, IV1-IV13: