# The Influence of Data Protection Regulation on the Information Security Culture of an Organisation - A Case Study Comparing Legislation and Offices across Jurisdictions

A. da Veiga

College of Science, Engineering and Technology, School of Computing, University of South Africa, UNISA, P.O. Box 392, 0003, South Africa
e-mail: dveiga@unisa.ac.za

## Abstract

The information security culture of an organisation is influenced by various factors, of which one could be related to legal and regulatory requirements. While employees must comply with organisational policies, external factors like data protection legislation might influence the manner in which employees protect information assets. This research sets out to investigate whether the information security culture level is consistent across offices of an organisation located in jurisdictions with and without data protection legislation and if the timeframe of the implemented data protection regulation might have had an impact. An information security culture survey was conducted in an organisation that follows a centralised approach to information security. Statistical analysis was conducted to compare the information security culture data of offices across six data protection jurisdictions where the organisation operates, namely Mauritius, Switzerland, Guernsey, South Africa, United Kingdom and Australia. It was found that the three offices (Mauritius, Switzerland and Guernsey), that had significantly more positive results, were all based in jurisdictions with implemented data protection legislation. However, the timeframe of the implemented data protection legislation did not seem to influence the information security culture mean scores, although the legislation incorporates the data protection principle of security. While data protection legislation might play a role to cultivate a more positive information security culture, other factors such as a large staff component could also play a role which can be further investigated.

## Keywords

Information security culture; data protection; legal; regulatory; centralised management, POPIA

## 1. Introduction

Employee behavior and interactions with organisational information and systems over time become the way things are done, as evident in the information security culture (Schlienger and Teufel, 2002; Da Veiga and Eloff, 2010; AlHogail, 2016). The information security culture of an organisation could be influenced by various factors, such as awareness (Connolly et al., 2017; AlHogail, 2016), management (Flores and Ekstedt, 2016; Sheriff et al., 2015), policies (Box and Pottas 2013; Sherif et al., 2015) as well as legal and regulatory requirements that could play a role

(AlHogail and Mirza 2015). Legal and regulatory requirements are incorporated in the Information Security Culture Frameworks of AlHogail (2015) and Da Veiga and Eloff (2010), who argue that external factors to an organisation, such as legal and regulatory systems, as well as internal factors like the information security policy, are critical components of an information security culture.

Organisations must comply with legal and regulatory requirements for the processing of information and should also ensure that their information security and data privacy policies are aligned to the relevant laws (ISO/IEC:27002, 2013). Multinational or international organisations often govern information security across the organisation through group policies, giving the minimum requirements for all their operations (offices) across legal jurisdictions. Some offices might be located in jurisdictions with stringent data protection laws, like Canada, Hong Kong, Austria and the United Kingdom (DLA PIPER, 2017; Greenleaf, 2014). Other offices might reside in jurisdictions that are in the process of enacting or implementing such laws, such as Namibia, Botswana, India and certain states in South America (DLA PIPER, 2017; Forrester, 2017; Greenleaf, 2014). Offices of organisations that are located in jurisdictions with limited or no data protection legislation have to abide by the internal compliance requirements of the organisation, from a policy or contractual perspective, although similar external compliance requirements might not be applicable to those offices.

The focus of this research is to determine if the information security culture level is consistent across offices of an organisation  located in jurisdictions with and without data protection legislation and if the timeframe of the implemented data protection regulation might have had an impact. This is researched within the context of an organisation following a centralised approach to the management of information security. This has not been researched through an empirical study before and, as such, data form a quantitative information security culture assessment of an organisation with offices across data protection jurisdictions was analysed to answer the research questions.

## 2. Research Questions

This paper aims to answer the following research questions:

For international organisations with a centralised information security management approach:

- Is the information security culture level consistent across offices?
- Is the information security culture level higher for offices located in jurisdictions with implemented data protection legislation, compared to offices that are not?
- Does the time frame of implemented data protection legislation of a jurisdiction where the organisation's office is situated have an impact on the level of information security culture of that office?

To answer the research questions the data protection legislation of the countries included in the sample are compared based on aspects such as whether the legislation is enacted, the timeframe that the legislation has been in place and the general data protection principles. The next section provides an overview of information security culture, followed by the comparison of the data protection legislation of the jurisdictions included in the scope. The research methodology and results are discussed thereafter.

## 3. Information Security Culture

There is no doubt that the human factor is regarded as a weak link in the protection of information security (Connolly et al., 2017; Tsohou et al., 2015; Chen et al., 2015). The Action Line C5 of the World Summit of Information Society (WSIS), Geneva Action Plan (2003), the Organisation of Economic Cooperation and Development (OECD, 2005) and numerous academic research (Parsons et al. 2017; Karlsson et al., 2016; Flores and Ekstedt 2016, Dhillon et al., 2016; Alhogail, 2015; Sherif et al., 2015) therefore focus on the development of an information security culture to aid in minimizing the risk that the human element poses to the protection of information.

An information security culture is defined by as the "attitudes, assumptions, beliefs, values and knowledge that employees/stakeholders use to interact with the organisation's systems and procedures at any point in time. The interaction results in acceptable or unacceptable behavior evident in artefacts and creations that become part of the way things are done in the organisation to protect its information assets" (Da Veiga and Eloff 2010). The information security culture of an organisation's offices located in different legal jurisdictions might vary, which would support the work of Hofstede (2010), who found that the values of national culture vary between countries. This would imply that the way things are done in the organisation to protect information could differ between offices located in different countries (or jurisdictions) as a result of different attitudes, assumptions, beliefs, values and knowledge of employees/contractors/service providers/suppliers/stakeholders as far as information security in that jurisdiction is concerned.

While the national culture and regulatory requirements could differ between offices of an organisation located across jurisdictions, all offices must comply with the information security policy in the organisation if a centralised approach for information security management is followed. A centralised approach for information security management has the advantage that the organisation has a comprehensive and consistent view of information security risk across the organisation (Harold 2007). In an organisation where the information security function is managed in a centralised manner, management (e.g. Country Security Officers) report to a centralised function and executive (e.g. Group Information Security Officer or Chief Information Officer) (Harold 2007). The centralised responsibility for information security together with factors such as a group information security policy aids in reducing conflict or different views or opinions on risks and threats to the organisation (Harold 2007). However, the information security culture might not be consistent across the offices of an organisation that follows a centralised approach due to various factors that could influence it, such as the national culture and data protection legislation of each jurisdiction.

### 3.1. The influence of regulatory requirements on the information security culture

AlHogail (2015) indicates that a number of external factors could affect the information security culture of an organisation, one being the legal and regulatory requirements and government initiatives. The scope of this research is limited specifically to data protection legislation as it incorporates the principle of information security. This principle is also covered by the Fair Information Principles (FIP, 2016) and the Guidelines on the Protection of Personal Information and Trans-border Flows of Personal Data of the (OECD, 2013), which were endorsed by the US Federal Trade Commission (FTC).

One of the OECD guidelines and FIP principles relate to information security measures that must be in place to protect the confidentially and integrity of personal information. The data protection principle of "security" is often included in data protection legislation and relates to the confidentiality and availability of information. The "information quality" principle of data protection relates to the integrity of information. Thereby, addressing the CIA-triad of information security. Organisations have to implement measures to protect personal information and employees have to comply with the security requirements of data protection legislation and internal organisational policies.

The perception and attitude of employees towards the implementation of information security in an organisation can be measured through an information security culture assessment which will provide an indication of the information security culture level in the organisation. The statistics derived from an information security culture assessment can be used for comparative purposes to better understand the information security culture of an organisation and the possible impact of data protection legislation on its offices located in different jurisdictions. This will enable the researcher to obtain quantitative data about the information security culture of the different offices of an organisation in order to compare the data between offices in different jurisdictions.

## 4. Data protection legislation overview for countries included in the case study

For this case study, offices of six jurisdictions where the organisation operates were compared, namely Mauritius, Switzerland, Guernsey, South Africa, United Kingdom and Australia. A high level overview of the data protection legislation in each of the jurisdictions is provided below with a comparison at the end focussing on general data protection principles.

### 4.1. Data protection legislation in South Africa

The Protection of Personal Information Act (POPIA, 2013) of South Africa was promulgated in 2013, but has not come into force as yet. Only the sections relating to the establishment of the Information Regulator are in force. The chairperson and members of the Information Regulator were appointed during 2016 to take office as of December 2016 (Information Regulator (South Africa), 2017). However, the commencement date of all sections of POPIA has not been announced.

### 4.2. Data protection legislation in Mauritius

The Data Protection Act (DPO, 2009) of Mauritius came into force in 2009. Mauritius has a Data Protection Office with a Data Protection Commissioner, Data Protection Officer Unit, Administrative, Cash Office Unit and IT Unit (Data Protection Commissioner Mauritius, 2017). The Data Protection Commissioner has published a number of guides and opinions, conducted awareness presentations, handled numerous complaints and issued the decisions thereof, such as unauthorized use of CCTV, disclosure of personal information, use of private e-mails and so on, and issued self-assessment and audit questionnaires (Data Protection Commissioner Mauritius, 2017).

### 4.3. Data protection legislation in Switzerland

In Switzerland, personal information is regulated by the Federal Act on Data Protection (FADP) of 1992 (FADP, 1992) as well as the Ordinance to the Federal Act on Data Protection (OFADP) of 1993 (OFADP, 1993). There are also 26 cantonal data protection acts applicable to the 26 Swiss cantons. Switzerland is not part of the European Union and therefore the General Data Protection Regulation (GDRP, 2016) does not apply to them. The Federal Protection and Information Commissioner (FDPIC, 2017) fulfils the role of the regulatory authority and publishes numerous guideline documents on their website, ranging from big data and surveillance in the workplace to privacy technologies.

### 4.4. Data protection legislation in Guernsey

Data protection in the Channel Islands is regulated through the Data Protection (Bailiwick of Guernsey) Law of 2001 (DPA, 2001). The Data Protection Commissioner of Guernsey (2017) acts as the independent statutory authority for the law. The Commissioner issues guidance for individuals about their rights and also guidelines for organisations to aid with compliance. Guernsey also has to comply with the GDPR (2016), being part of the European Union.

### 4.5. Data protection legislation in the United Kingdom

The processing and protection of personal data in the United Kingdom is governed by the Data Protection Act (DPA) of 1998 (DPA, 1998), which came into effect in March 2000. Compliance is regulated by the Information Commissioner's Office

(ICO, 2017). The United Kingdom is also preparing for compliance with the GDPR (2016), which will commence in 2018 (ICO Information Commissioners Blog, 2016). The ICO is active in the United Kingdom and has published various guidelines for organisations and individuals. The office has ruled on more than 8,500 related cases and actively audits and monitors organisations for compliance. Their website also allows for the reporting of concerns.

### 4.6. Data protection legislation in Australia

In Australia, the processing of personal information is regulated by the Federal Privacy Act 1988 (Privacy Act, 1988) as well as data protection legislation of the states and territories. The regulatory authority for the Privacy Act is the Australian Privacy Commissioner which is integrated within the Office of the Australian Information Commissioner (OAIC, 2017). The OAIC has published various awareness material on their website, including guides for Privacy Impact Assessments, guides for securing personal information and breach notification, and fact sheets. It also provides a platform for complaints. Determinations of court cases are also published on the OAIC website.

### 4.7. Comparison

Table 1 provides a comparison of the data protection legislation of the countries in the sample compared with the data privacy principles of the FIP and the OECD. The categories in the first row relates to research work conducted by Botha et al. (2017). Collection limitation was added to ensure that all the FIP and OECD privacy principles are included, which are covered by all the acts listed in table 1. Sensitive personal information and direct marketing were also added for a more comprehensive comparison. The Y" indicates that a principle is covered by an act.

Accountability and online privacy seems to be lacking in most of the acts included in the scope, followed by breach notification and further processing. Breach notification was introduced to the Privacy Act in Australia in October 2016 (DLA PIPER, 2017). In the UK the Privacy and Electronic Communications Regulations of 2003 requires that organisations notify the ICO in the event of a data breach of personal data, however the DPA does not include it (DLA PIPER, 2017). Some regulations such as that of the UK and Australia include cookie compliance under online privacy whereas Switzerland covers online privacy in the Swiss Telecommunications Act (DLA PIPER, 2017). The data protection legislation in the United Kingdom and Australia are regarded as "Heavy" (red), whereas Switzerland is "Moderate" (orange) and South Africa, Mauritius and Guernsey are regarded as "Low" (yellow) in terms of the regulation requirements and enforcement (DLA PIPER, 2017).

The data protection regulations of all five the countries in table 1 include security and information quality in their data protection legislation to ensure the confidentiality, integrity and availability of personal information by data controllers and processors. Therefore allowing for a comparison related to the implementation of the information security requirements as evident in the information security culture.

| Country | Act / Standard | Accountability | Processing / Use Limitation | Collection limitation | Purpose Specification | Further Processing Limitation | Information Quality | Openness | Security Safeguards | Data Subject Participation/ Access | DPO /IO Required | Breach Notification | Cross-border Data Transfer Limitations | Direct marketing | Online Privacy | Sensitive personal information | Commencement Year (all sections) | Number of years to 2013 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **FIP** | Y | Y | Y | Y | | **Y** | Y | **Y** | Y | | | | | | | | |
| | **OECD** | Y | Y | Y | Y | | **Y** | Y | **Y** | Y | | | | | | | | |
| **South Africa** | POPIA | Y | Y | Y | Y | Y | **Y** | Y | **Y** | Y | Y | Y | Y | Y | | Y | TBD | 0 |
| **Mauritius** | DPA | | Y | Y | Y | Y | **Y** | Y | **Y** | Y | Y | | Y | Y | | Y | 2009 | 5 |
| **Switzerland** | FADP<br>DPO | | Y | Y | Y | | **Y** | Y | **Y** | Y | Y | | Y | | | Y | 1992 | 22 |
| **Guernsey** | DPO | | Y | Y | Y | Y | **Y** | Y | **Y** | Y | Y | | Y | Y | | Y | 2001 | 13 |
| **United Kingdom** | DPA | | Y | Y | Y | Y | **Y** | Y | **Y** | Y | Y | | Y | Y | | Y | 2000 | 14 |
| **Australia** | PA | | Y | Y | Y | | **Y** | Y | **Y** | Y | Y | Y | Y | Y | | Y | 1988 | 26 |
| **European Union** | GDPR | Y | Y | Y | Y | Y | **Y** | Y | **Y** | Y | Y | Y | Y | Y | Y | Y | TBD | 0 |

**Table 1: POPIA data privacy principle comparison with data privacy legislation in selected countries and standards (OECD, 2013; FIP, 2017; POPIA, 2013; DPA Mauritius, 2009; FADP, 1993; DPO Swiss, 1993; DPO Guernsey, 2001; DPA UK, 1998; Privacy Act, 1988; GDPR, 2016; DLA PIPER 2017; Botha et al., 2017)**

## 5. Research Methodology

A case study methodology was applied using quantitative methods, including statistical analysis (Sanders and Lewin 1990). In the context of a case study, a single social unit is studied in depth with intensive analysis in the context of the research problem being investigated (Blaikie 2010). A survey method was used whereby a systematic instrument, such as a questionnaire, is used to gather data from a sample of a population which is analysed with statistics (Lavrakas 2008). While surveys are a cost-effective manner to conduct research, it also has the benefit of including large samples of users to participate (Brewerton and Millard, 2002, Lavrakas 2008). However, care should be taken to ensure that the sample is representative and that the measuring instrument produces reliable and valid data (Brewerton and Millward 2002). These aspects were considered as part of the research and are discussed in the sections below. For the purpose of this research, an information security culture survey was conducted. The data derived was used to conduct comparative analysis between six offices of the organisation in this study. The next section gives an overview of the organisation, questionnaire and responses required.

### 5.1. Organisation

The survey was conducted in a global organisation. The organisation follows a centralised approach for the management and implementation of information security and data privacy policies. The organisation therefore has a global information security policy and related procedures that all operations have to comply with as the minimum standard. There are information security officers in the various jurisdictions who report to a group information security officer.

### 5.2. Measuring instrument

The Information Security Culture Assessment (ISCA) (Da Veiga and Martins 2015) questionnaire was utilized for this research. The ISCA is a validated questionnaire with an internal reliability score of between 0.764 and 0.877 (Da Veiga and Martins 2015), measuring the perception and attitude of employees towards information security in an effort to determine the information security culture. While other information security culture instruments exist such as that of Schlienger and Teufel (2002) or AlHogail (2015), the ISCA was selected as it is valid and reliable and the researcher developed and applied it in previous research in the case study organisation.

The ISCA questionnaire comprises three sections, namely, a knowledge section where 18 questions are used to obtain an understanding of general information security awareness, a second section with 55 information security culture statements answered on a five-point Likert scale and the third section with a number of demographical questions. Where the mean of the information security culture statements is above 4.00, it is regarded as a positive information security culture. If, however, the mean score is below 4.00, actions should be implemented to address developmental constructs or statements, as identified in the survey data. The information security culture section includes eight constructs, namely, information asset management, information security policies, change, user management, information security program, information security leadership, information security management and trust.

Survey Tracker (2017) software was used to develop the questionnaire in electronic format, to collect and analyze the data. In addition, the Statistical Package for the Social Sciences (SPSS) (2013) was used to conduct the significant difference analysis using the one-way analysis of variance (ANOVA) test.

## 6. Results

The overall information security culture mean for the organisation was 4.10, indicating a positive or strong information security culture. The results of the survey are discussed below, focusing on the overall mean scores of the information security culture questions. The results are reported, starting with the response rates and results per office in each jurisdiction, followed by a discussion of the results in line with each research question.

## 6.1. Responses

Responses from the organisation's offices across six jurisdictions, namely, Australia, Guernsey, Mauritius, South Africa, Switzerland and the United Kingdom, were included in the scope. The data of these six offices were found to differ significantly from each other based on ANOVA tests. The Ireland and Jersey office data were excluded from the analysis, as no significant differences were identified between these offices and the other offices; it was thus not significantly more negative or positive. The offices that could not be included due to receiving fewer than three responses were located in Botswana, Hong Kong, Namibia and the office in the United States. Table 2 outlines the number of responses obtained per office in each respective jurisdiction.

The Mauritius, Switzerland and Guernsey offices had smaller numbers of staff employed and hence a smaller number of responses for the survey when compared with the offices in South Africa, the United Kingdom and Australia. For example, while the Switzerland office only had 15 responses, it represented a 29% response rate as the office employs fewer staff compared to the Johannesburg office, where 587 responses were obtained, representing a 23% response rate. A total of 2 159 responses were obtained from the organisation's employees. On a 95% confidence level only 367 responses were required, based on the method of Krejcie and Morgan (1970). Thus, an adequate number of responses were obtained.

| **Office** | **Survey responses received** | **ISCA mean** | **Data protection legislation in place** |
|---|---|---|---|
| Mauritius office | 57 | 4.49** | Yes |
| Switzerland office | 15 | 4.35** | Yes |
| Guernsey office | 39 | 4.34** | Yes |
| South Africa office | 587 | 4.07* | No |
| United Kingdom office | 600 | 4.05* | Yes |
| Australia office | 167 | 4.04* | Yes |

**Table 2: Responses per office in each respective jurisdiction and ISCA mean**

## 6.2. Research question 1

*Is the information security culture level consistent across offices?*

ANOVA tests were used to identify the offices that scored significantly higher than the lowest scored offices. Table 2 lists these offices with the corresponding mean for the information security culture questions (section two of the questionnaire). The results for offices located in Mauritius, Switzerland and Guernsey were significantly more positive (**) than those for the three offices with the lowest mean (*), namely the office in South Africa, United Kingdom and Australia.

The information security culture level is therefore found not to be consistent across the offices of an organisation that follows a centralised approach to information security culture. This could be related to various factors such as internal management of country security officers, subcultures or the number of staff employed in a respective office, which requires further research.

### 6.3. Research question 2

*Is the information security culture level higher for offices located in jurisdictions with implemented data protection legislation, compared to offices that are not?*

The six offices are each located in a different jurisdiction, which enables a comparison when considering the data protection legislation of those jurisdictions. Column three of table 2 indicates whether the respective office is in a jurisdiction with implemented data protection legislation or not. Of the jurisdictions in the study, only South Africa did not have implemented data protection legislation at the time of the survey.

Data protection legislation has been implemented in Mauritius, Switzerland and Guernsey. These three offices have a higher information security culture score than South Africa, where data protection legislation has not yet been implemented. However, the offices in the United Kingdom and Australia scored lower than the South African office, despite having data protection legislation and despite being classified as countries with "heavy" data protection legislation.

From the results one cannot conclude that the information security culture level is higher for offices located in jurisdictions with implemented data protection legislation, compared to jurisdictions where it is not. However, one can conclude that the offices that scored significantly higher are all located in jurisdictions with implemented data protection legislation. This answers research question two, however, further investigation is required to establish whether or not the role that the government, information commissioners and national culture play might have had an influence.

### 6.4. Research question 3

*Does the time frame of implemented data protection legislation of a jurisdiction where the organisation's office is situated have an impact on the level of information security culture of that office?*

Figure 1 shows the number of years that data protection legislation has been in place in each of the jurisdictions up to 2013, when the case study data was collected. The information security culture mean is depicted on the secondary X-axis. The mean varies for the offices located in jurisdictions with implemented data protection legislation. Australia, where the DPA has been in place for 26 years, has the lowest information security culture mean for the organisation included in this study. Switzerland, that has had the FADP in place for 22 years, scored the second highest information security culture mean. The United Kingdom, that has had the DPA in place for 16 years, scored lower than South Africa, where POPIA has not yet commenced.

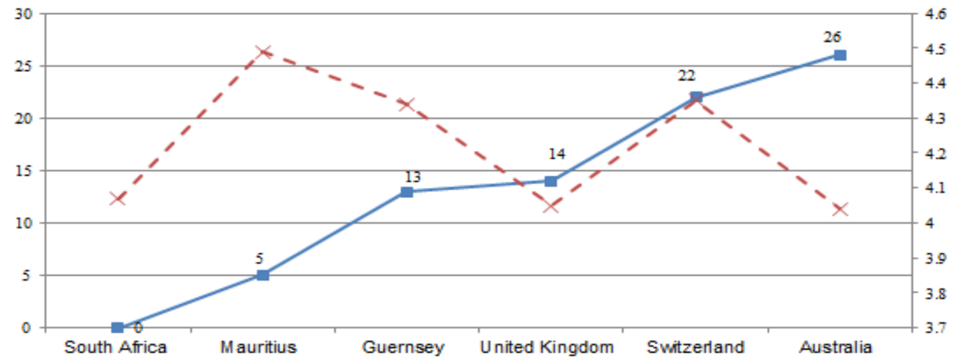

**Figure 1: Mean per office including years that data protection legislation had been in place (Striped red line: mean, Solid blue line: years)**

From the results there does not seem to be a correlation between the information security culture mean score and the number of years that the data protection legislation has been in place in the organisation used in this study. This answers the third research question.

If one considers the responses obtained per office compared with the information security culture mean score (see table 2) it seems as though the information security culture mean score is higher for the offices with smaller staff numbers and lower for offices with larger staff numbers. The Mauritius, Switzerland and Guernsey offices, that employ small numbers of staff, were found to be significantly more positive than the larger offices, namely Australia, South Africa and the United Kingdom. Therefore, additional interventions, such as additional training, awareness and monitoring activities, might be required for offices with a large staff component. This is an aspect that could be further investigated in future research.

## 7. Limitations and Future Research

A limitation of the study is that the data of only one organisation were used. From this organisation’s operations only one office from a jurisdiction with pending data protection legislation, namely South Africa, could be included in the analysis, as other offices, such as Botswana, did not have a representative response rate to include it in the analysis. To further investigate the influence of data protection legislation on the information security culture, additional organisations should be included in the sample, and specifically organisations with a number of operations across jurisdictions with and without data protection legislation. Organisations that follow a decentralised approach to the management of information security and data privacy should also be included in future research.

## 8. Conclusion

The objective of this research was to establish whether data protection legislation might influence the information security culture level across offices of an international organisation, following a centralised approach for information security management. A case study was conducted in an organisation where an information security culture survey was conducted to derive data that could be used for comparison purposes. Six offices across six different jurisdictions were included in the analysis, namely, Mauritius, Switzerland and Guernsey, South Africa, the United Kingdom and Australia.

The results indicated that the information security culture level of the organisation varied between its offices despite following a centralised approach for information security management. The information security culture did not seem to be influenced by the presence or absence of implemented data protection legislation, although the data protection legislation included the principles of security and integrity. However, all three offices whose scores were significantly more positive than the three lowest scored offices were located in jurisdictions with implemented data protection legislation. It was found that the time frame of implemented data protection legislation did not seem to impact on the level of information security culture in the context of the organisation in this study. However, offices with smaller staff numbers had a more positive information security culture compared to offices with large staff numbers. Future research will concentrate on including more organisations across various jurisdictions in the sample to further compare the influence of the data protection regulation on the information security culture.

## 9. References

Action Line C5 of the World Summit of Information Society (WSIS). (2017), "Geneva Action Plan", http://www.itu.int/net/wsis/documents/doc_multi.asp?lang=en&id=1161|0 (Accessed 28 February 2017).

AlHogail, A. (2015), "Design and validation of information security culture," *Computers in Human Behaviour*, Vol. 49, pp. 567-575.

AlHogail, A., and Mirza, A. (2015), "Organisational information security culture assessment," in The 2015 World Congress in Computer Science, Computer Engineering and Applied Computing (SAM'15) proceedings, Las Vegas, pp. 287–292.

Blaikie, M. (2010), *Designing social research*, 2nd edn., Polity Press: Cambridge.

Botha, J., Grobler, M. M., Hahn, J. and Eloff, M. (2017), "A High-Level Comparison Between the South African Protection of Personal Information Act and International Data Protection Laws," in *International Conference on Cyber Warfare and Security Conference Proceedings*, p. 57.

Box, D. and Pottas, D. (2013), "Improving information security behaviour in the healthcare context," *Procedia Technology*, Vol. 9, pp. 1093–1103.

Brewerton, P. and Millward, L. (2002), *Organisational research methods*. London: Sage Publications.

Chen, Y., Ramamurthy, K., and Wen, K. (2015), "Impacts of comprehensive information security programs on information security culture," *Journal of Computer Information Systems*, Vol. 2015, No. 55, pp. 3-11.

Connolly, L.Y., Lang, M., Gathegi J., Tygar, D.J. (2017), "Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study", *Information & Computer Security*, Vol. 25 Issue: 2, pp.118-136.

Da Veiga, A. and Eloff, J.H.P. (2010), "A framework and assessment instrument for information security culture," *Computers & Security, V*ol. 2010, No. 29, pp. 196-207.

Da Veiga, A. and Martins N. (2015), "Improving the information security culture through monitoring and implementation actions illustrated through a case study", *Computers & Security*, Vol. 2015, No. 49, pp. 162-176.

DLA PIPER. (2017), Data protection laws of the world, https://www.dlapiperdataprotection.com/index.html (Accessed 15 August 2017).

Data Protection Act (PDA) of the United Kingdom. (1998), http://www.legislation.gov.uk/ukpga/1998/29/contents (Accessed 15 August 2017).

Data Protection Act 2004 of Mauritius, Act 13 of 2004. (2004), Data Protection Office, http://dataprotection.govmu.org/English/Documents/The%20Law/DPOregul.pdf (Accessed 15 August 2017).

Data Protection Commissioner Mauritius. (2017), http://dataprotection.govmu.org/English/Pages/default.aspx (Accessed 15 August 2017).

Data Protection Commissioner of Guernsey. (2017), https://dataci.gg/about-us (Accessed 15 August 2017).

Dhillon, G., Syed R. and Pedron, C. (2016), "Interpreting information security culture:

An organizational transformation case study", *Computers & Security*, Vol. 2016, No. 56, pp. 63-69.

Faily, S. and Fléchais, I. (2010), "Designing and aligning e-science security culture with design", *Information Management and Computer Security*, Vol. 18, No. 5, pp. 339-349.

Fair Information Practice Principles (FIP). (2017), IT Law Wikia, http://itlaw.wikia.com/wiki/Fair_Information_Practice_Principles (Accessed 15 August 2017).

Federal Protection and Information Commissioner (FDPIC) of Switzerland, (2017), https://www.edoeb.admin.ch/?lang=en (Accessed 15 August 2017).

Flores, R. and Ekstedt, M. (2016), "Shaping intention to resist social engineering through transformational leadership, information security culture and awareness", *Computers & Security*, Vol. 2016, No. 59, pp. 26-44.

Forrester. (2017), Privacy and Data Protection by Country, for security and risk professionals, http://heatmap.forrestertools.com/ (Accessed 15 August 2017).

General Data Protection Regulation (GDPR). (2016), http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (Accessed 15 August 2017).

Greenleaf, G. (2014), "Scheherazade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories," *Journal of Law, Information & Science*, Vol. 23, No.1, pp.1-48.

Harold, F.T. and Krause, M. (2007), *Information Security Management Handbook*, 6th ed., Taylor and Francis: Roca Raton.

Hofstede, G., Hofstede, G.J. and Minkov M. (2010), *Cultures and organisations: software of the mind*, 3rd ed. McGraw-Hill: New York.

ICO Information Commissioners Blog. (2016), How the ICO will be supporting the implementation of the GDPR, https://iconewsblog.wordpress.com/2016/10/31/how-the-ico-will-be-supporting-the-implementation-of-the-gdpr/ (Accessed 15 August 2017).

Information Commissioner's Office (ICO). (2017), https://ico.org.uk/, (Accessed 28 February 2017).

Information Regulator (South Africa). (2017), http://www.justice.gov.za/inforeg/index.html, (Accessed 15 August 2017).

ISO/IEC 27002:2013. (2013), *Information technology - Security techniques - Code of practice for information security management*, The British Standards Institute.

Karlsson, F., Åström, J., and Karlsson, M. (2016), " Information security culture – state-of-the-art review between 2000 and 2013", *Information & Computers Security*, Vol. 2, No. 3, pp. 246-278.

Krejcie, R.V. and Morgan, D.W. (1970), "Determining sample size for research activities," *Education Psychology Measurement*, Vol. 1970, No. 30, pp. 607-610.

Lavrakas, P.J. (2008), *Encyclopaedia of Survey Research Methods*, Sage Publications Inc.

OECD (Organisation for Economic Cooperation and Development). (2005), *The promotion of a culture of security for information systems and networks in OECD countries*, http://www.oecd.org/internet/ieconomy/35884541.pdf (Accessed 15 August 2017).

Organisation of Economic Cooperation and Development (OECD). (2013), *OECD privacy principles,* https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (Accessed 15 August 2017).

Office of the Australian Information Commissioner (OAIC). (2017), https://www.oaic.gov.au/ (Accessed 15 August 2017).

Ordinance to the Federal Act on Data Protection (DPO). (2017), The Federal Council, The portal of the Swiss government, https://www.admin.ch/opc/en/classified-compilation/19930159/index.html (Accessed 15 August 2017).

Parsons K., Calic, D., Pattinson, M., Butavicius M., McCormac and A., Zwaans T. (2017), "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies", *Computers & Security*, No. 2017, Vol. 66, pp. 40-51.

Privacy Act, Act No. 119 of 1988. (1988), The Parliament of Australia, https://www.legislation.gov.au/Series/C2004A03712 (Accessed 15 August 2016).

Protection of Personal Information Act (POPIA) 4 of 2013, Vol. 581, No. 37067. (2013), Cape Town, South Africa, http://www.justice.gov.za/legislation/acts/2013-004.pdf (Accessed 15 August 2017).

Schlienger, T. and Teufel, S. (2002), "Information security culture. In *Security in the Information Society Proceedings*, IFIP/SEC2002, Boston: Kluwer Academic, pp. 191-201.

Sherif, E., Furnell, S. and Clarke, N. (2015), "An identification of variables influencing the establishment of information security culture," in Tryfonas T, Askoxylakis I, Eds. The human-computer interaction (HCI) conference - human aspects of information security, privacy and trust (HAS), Switzerland, Springer, pp. 436–448.

SPSS. (2013), Version 22. Licensing, 200 W, Madison St. Chicago, IL, 60606, U.S.A: IBM Software Group, ATTN.

Survey Tracker. Training Technologies Inc. (2017), http://www.surveytrackersoftware.com/ (Accessed 15 August 2017).

The Data Protection (Bailiwick of Guernsey) Law. (2001), http://www.guernseylegalresources.gg/article/94296/Data-Protection-Bailiwick-of-Guernsey-Law-2001 (Accessed 28 February 2017).

The Federal Act on Data Protection (FADP). (1992), The Federal Council, The portal of the Swiss government, https://www.admin.ch/opc/en/classified-compilation/19920153/index.html (Accessed 15 August 2017).

Tsohou, A., Karyda, M. and Kokolakis, S. (2015), "Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programmes", *Computers & Security*, Vol. 2015, No. 52, pp. 128-141.