POL00227400

Confidential

Second Sight Support Services
Third Party Assurance Review
Annex A

Site Visit Overview

Attendees: Claire Davies (Post Office Certified ISA Auditor)
Ron Warmington (Director: Second Sight Support Services)
Ian Henderson (Director: Second Sight Support Services)

Site Visited: Tythe Farm (Private Residence)

Date: 24 Jun 2014

Executive Summary

Second Sight Support Services (SS) are not aligned to an international information security standard; however they appeared to demonstrate sound best practice by incorporating information security into their working environment. There is work to be done on the method of communicating information, particularly between applicants and SS. Whilst these could be implemented without too much difficulty or resource, it is accepted that most of the information has already been collected by SS and therefore the risk of compromise between the applicant and SS in reduced.

During the review, five non-conformities were identified and four security weaknesses; these are detailed in Annex A to this report. When considering impact to the business and likelihood of a non-conformity or security weakness being exploited by a threat agent, SS is considered of MEDIUM risk to the business.

Service Provided

Post Office employed the services of SS to carry out a review into alleged problems with the Horizon System. Mr Warmington, Director of SS was known to Sue Crighton, the previous General Council, after working together in General Electric and was recommended as a preferred bidder[1].

[1]It was noted, SS presented a more "human face" for this sensitive task compared to the popular 'Big 4' corporate audit companies: PWC, EY, Deloitte and KPMG.

POL00227400

During June and July 2012, the Scope was discussed with Post Office Senior Management, the Rt Hon James Arbuthnot MP[2] and with Alan Bates and Kay Linnell representing the Justice for Subpostmasters Alliance, following which the remit of the Inquiry was later defined[3] as:

> "to consider and to advise on whether there are any systemic issues and/or concerns with the Horizon system, including training and support processes, giving evidence and reasons for the conclusions reached".

It was also agreed that SS interim reporting would:

> "report on the remit and if necessary will contain recommendations and/or alternative recommendations to Post Office Limited relating to the issues and concerns investigated during the Inquiry. The report and recommendations are to be the expert and reasoned opinion of Second Sight in the light of the evidence seen during the Inquiry."

Initially, Post Office gave SS approximately twenty criminal cases brought against Sub-Postmasters (SPMRs) who were accused, and subsequently found guilty, of criminal offences. This task has since morphed, to include providing a single point of contact (SPOC) for SPMRs and ex-SPMRs (hereafter known as applicants) to request an independent review of their cases. To date, c150 applicants have registered their cases. SS have recently started providing summary reports on each case to the Mediation Group and intend to continue this pace of providing 3-4 reports per week for approximately 12-15 months. SS routinely attend, monthly progress meetings, via conference call, with the Mediation Team and weekly to the larger Mediation Working Group.

Business Overview

Both Mr Warmington and Mr Henderson maintain membership of the Institute of Chartered Accountants which requires them to provide annual returns to ensure, among other things, that the principles of information security are practiced. Mrs Warmingon and a sub-contractor, Mr Holyoak also has access to Post Office and applicant information. Whilst Mr Henderson is a Director in SS, for the purpose of the Post Office account, his work is undertaken by his Advance Forensics company.

[2] Rt Hon James Arbuthnot MP was, and has remained, the parliamentary lead for addressing allegations brought by constituents who questioned the integrity of the Horizon system

[3] SS Interim Report into alleged problems with the Horizon system dated 8 Jul 2013.

POL00227400

SS's email service is supplied by Organisation Evil Attitude Ltd based in Redcar and hosted by Easyspace Ltd, Glasgow. Their website is registered to Fast Hosts Internet Ltd, Discovery House, 154 Southgate Street, Gloucester, GL1 2EX. The SS website provide a webpage for Post Office Mediation, signposting applicants via email to the company Directors and a group email account mediation GRO which flows through to Mr and Mrs Warmington, Mr Henderson and Mr Chris Holyoak.

During the initial stages of the Mediation scheme, Post Office information was passed to SS by FileSafe, Royal Mail Special Delivery, encrypted removable hard drives[4] and compact disks. As the scope of the service has expanded the method of information sharing has also developed alongside. Currently the Mediation Working Group uses a commercially available secure application, 'Huddle', for this purpose. Applicants generally use email, signposted from the webpage to contact SS. A small amount of items are sent to SS in hardcopy format, either by the Post Office or from applicants, and on receipt they are transferred to electronic format and hardcopy security destroyed.

SS process information on business owned[5] laptops; each has full disk encryption to "CESG standard"[6]. Information is stored in a logical manner and segregated from other clients. Data is subject to daily incremental back-up on the laptops and full weekly back-up to an encrypted iStorage removable hard drive held by Ian Henderson at his office at Omnibus Business Centre, 39-41 North Road, London N7 9DP. SS retain a number of CDs at Tythe Farm which are stored in a locked security cabinet[7] on the premises. Destruction of data and devices takes place on site, using CESG wipe tools, commercial cross-cut shredder and/or incineration. Provision for deploying an exit strategy by purge for all client and applicant data is available on request.

[4] During the site visit on 24 Jun 2014 the auditor recovered a iStorage device which was no longer required by SS
[5] Either SS or Advanced Forensics working as the sub-contractor to SS.
[6] Quote from Ian Henderson
[7] This cabinet was not observed during the Audit.

POL00227400

Confidential

Second Sight Support Services
Third Party Assurance Review
Annex A

Recommendations for Improvement

The following observations and recommendations were noted during the Audit. This table does not provide an exhaustive list of the assessment, only the identified non-conformities[1] (NC) or security weakness[2] (SW). Should further information be required please contact Claire Davies in the Post Office Information Security Assurance Group (ISAG).

Where detailed, observations were discussed with SS and a security improvement measures agreed.

ID	Level	Observation	Recommendation	Proposed Owner
001	NC	At the time of Audit, SS had not signed a contract with the Post Office for the services they have been required to undertake. Whilst a contract was drafted, there was some dispute whether SS were Data Controllers or Data Processors.	A suitable supplier contract should be drafted and signed[3] between Post Office and SS. Given the scope of service provided by SS has changed from the original requirement to include collecting information direct from applicants, SS should be considered Data Controllers[4].	Mediation

[1] A non-conformity is a failure to adhere to legal, regulatory, ISO27001 and/ or Post Office policy requirements.
[2] A security weakness is failure to follow information security best practice within the industry.
[3] On 1 Jul 2014, an engagement letter was signed between Post Office and SS
[4] A view held by the Post Office Data Protection Officer

POL00227400

002	SW	Mr Warmington and Mr Henderson have signed separate Non-Disclosure Agreements. A third person, currently employed as a contractor to SS, Chris Holyoak, may become a Director of SS, in which case the SS intent is for him is to sign a separate NDA with Post Office.	SS should be required to sign a single NDA which will cover the services they provide to the Post Office. They should manage and be liable for their own employees and supply chain.	Mediation
003	NC	SS are registered with the ICO as a Data Controller #Z3440411. The description of services they provide is under General Business which is not a true reflection of all the services they provide to the Post Office. Failure to register, use the correct description or maintain your profile is considered a breach of DPA.	SS should review their ICO registration with a view to selecting a more appropriate business description or, if necessary, creating a bespoke entry. This point was raised during the audit. SS have provided evidence of contacting the ICO.	Mediation/SS
004	SW	SS is not aligned to any Information Security Standard.	SS should consider embedding the newly released Government Cyber Essentials Assurance Framework throughout the company. It provides a clear statement of the basic controls smaller organisations such as SS should implement to mitigate the risk from common internet based threats.	Mediation/SS
005	NC	SS do not maintain a register of information assets.	SS should initiate and maintain a register to ensure they are able to recognise assets, identify responsibility, location and, when necessary, destruction method for audit purposes.	Mediation/SS

POL00227400

006	NC	During the service period, Post Office and SS staff, have used both official and private[5] email accounts for communicating information. As a result of a recent incident, where Mr Warmington's AOL account was hacked, Post Office and the personal accounts of our staff received phishing emails. The use of private accounts is a breach of Post Office policy both internally and within our supply chain. It makes Data Loss Prevention of sensitive information difficult to control and presents an unnecessary threat to our information and systems. In addition, there is a threat that personal email accounts can be accessed by family members who are not authorised to view Post Office information.	In accordance with Policy, Post Office and SS staff must only use official email accounts for communicating official information. SS agreed to only use @2ndsight.eu accounts, going forward, for communicating information to Post Office and applicants.	Post Office /SS

[5] cJun 2013, SS interim report was sent to Susan Crichton personal email account allegedly because they had experienced problems with emailing the Post Office domain. A similar email failure occurred which resulted in Belinda Cortes-Martin passing her personal account details to Ron Warmington in order to test the email delivery. Allegedly following receipt of the email on one occasion, Ron used this account to send sensitive information and was warned at the time this action was considered a breach of Post Office policy.

POL00227400

007	NC	SS provide a SPOC for applicants to contact them via details on their website. There is potential that: • A malicious hacker could deploy website spoofing in an attempt to redirect applicants and collect information for nefarious purpose. • Sensitive information relating to cases including Personal Identifiable Information (PII), other than that of the applicant, could be communicated over the internet without any associated security controls and therefore be subject to man-in-the-middle attacks. These represent a risk to the confidentiality, availability and integrity of information and, given that SS are contracted to the Post Office, a reputational risk to the business and that of the applicant. Further to this, it could be considered a breach of Principle 7 of the DPA.	In order to negate the risk from website hacking, SS should consider utilising Hypertext Transfer Protocol Secure (HTTPS) for their website or just the Mediation page. To mitigate the risk of man-in-the-middle attacks on communications between SS and applicants, during the initial contact phase, consideration should be given to: • Providing a statement on the webpage warning applicants not to include sensitive information in the initial contact to SS; or • Implementing a secure web-based form within the backend application to provide for secure transfer of information. The form should be protected against script injection and other risks associated with embedded forms. The form should be transported to SS in a secure manner. All subsequent communications between SS and applicants should be suitably protected: • Only limited information should be sent within the body of an email.	Mediation/SS

POL00227400

			• Sensitive information should be sent as attachments, at least password protected, or at best encrypted. Passwords and/or keys should be sent via an alternative channel. • To prevent non-conformance, applicants should be advised on appropriate method of communication along with reasons for adopting these measures.	
008	SW	The Post Office Mediation page on SS's website provides numerous contact points for applicants: • Mediation group account • Mobile phone • Ron Warmington • Ian Henderson • David Jeffries Multiple contact points may be deemed confusing to the applicant and/or present an information management issue for the SS. Further to this, during the audit, David Jeffries was not listed as working on the Post Office account.	SS should consider only listing the group account and phone number as mediation contact points. If it is considered necessary to list individual contacts, and it is the case that David Jeffries does not work on the Post Office account, his details should be removed from the webpage.	Mediation/SS

POL00227400

009	SW	SS have been providing a service to the Post Office for nearly 2 years during which time the above mentioned potentially unnecessary risks have existed. When considering the timeliness of the service required, consideration should always be given to adopting adequate security measures from the onset to ensure information is protected through the lifecycle of the service.	Should there be a future requirement to use the services of a sole trader or small company who do not enjoy the experience or resources of a larger business, appropriate due diligence should be conducted beyond just legal contracts. The subsequent security improvement plans should be agreed upon and deployed prior to the service launch.	Mediation/Com Sec

Confirmation is required on closure of the above recommendations. No further assessment will be required unless there is a change in the provisions of services from SS in which case ISAG should be notified.