Research New Zealand – Data and Sample Security Policies and Practices

Introduction

Given our Wellington-based location and our largely public sector client base, we have focused our data and sample security policies and practices on meeting the requirements identified in the **New Zealand Information Security Manual** (NZ ISM)[1].

Specifically, our data and sample security policies and practices reflect the fact that our clients typically provide us with customer information that is considered to be in-confidence, potentially sensitive and /or restricted (i.e. contact details and administrative information). As such, our data and sample security policies and practices are aimed at meeting the essential or minimum acceptable levels of control as covered under Section 16 of the NZ ISM.

Files containing confidential customer information

We have developed policies and practices to ensure that **files received from and data repatriated to clients** containing confidential information are not compromised.

We prefer to receive files of confidential administrative information provided by clients for the purposes of completing their research projects (e.g. files containing the names and contact details of customers) in an **encrypted, password protected form, through to a dedicated SharePoint client portal**.

We recommend our clients use this secure client portal to provide and receive confidential files and only in exceptional cases will we agree to receive files on a memory stick for example. In these cases, the files must be **encrypted, password protected.**

If, in addition to contact names and details, other administrative information is included on a file, we ensure this is the **absolute minimum required** for the purposes of the project. In some cases, client administrative data is provided to us as coded categorical numerics without any descriptive labels, to further assure any information of a sensitive nature is not personally identifiable by us.

As soon as a file is received, a 'working copy' of it is created. This ensures that any work completed on the file (e.g. to prepare for a mail out) does not run the risk of corrupting the original file and a master is always available for checking purposes.

Survey data relating to a respondent's identity is removed from any administrative information that is held on that respondent as soon as is practically possible following the completion of the interviewing for a project (i.e. **the survey data is de-personalised**). This is a requirement under the Codes of Practice of the European Society for Marketing & Opinion Research (ESOMAR) and Research Association of New Zealand Inc. (RANZ).

[1] The New Zealand Information Security Manual has been published by the Government Communications Security Bureau (December 2014).

When a project has been completed, the file of administrative information (including copies) relating to that project is either **returned to the client or destroyed**, and the client advised so. This is also a requirement under the Codes of Practice of ESOMAR and RANZ.

Access control

Access to client provided files and data is **restricted to those researchers working on the project** that the file relates to. If **telephone interviewers** are involved in the project, they are only provided the information they require in order to identify and establish contact with a given respondent. **All other information is withheld from the interviewers**.

Specific policies and practices relating to access control are as follows:

- Our current password policy and practices compliant under the relevant NZ ISM Section 16 MUST System Classification Control. These cover our staff's:
  - Identification.
  - Authentication.
  - Authorisation.
- Our internal computer network uses a combination of **physical, virtual and logical segregation practices**.

  From the top down, our network is organised into a **number of different physical servers**.
  - Two of these physical servers host the Hyper-V virtual servers where data and research project specific files are held.
  - At the next level down, network files are organised within SharePoint™, based upon a logical top-down segregation system of Client (i.e. Inland Revenue), Customer Groups (as defined by each client), research project (e.g. the CS&P), etc.
  - Our Web Server and Data Collection servers (IBM Data Collection, SQL servers) are virtual machines that are hosted with New Zealand's leading local Cloud Infrastructure and Services company, Revera. These servers also host our client accessible digital dashboard reporting tools.

    As part of their service, Revera apply 'defence in depth' principles to network security. These protect Research New Zealand data from unauthorised external access and include:
    - continuous gateway security intrusion prevention and detection testing,

- including the automatic scanning of external firewall ports for changes that may have introduced vulnerabilities.

In addition, Revera maintains a single information security management system, to comply with All of Government IaaS security requirements and align with AS/NZS ISO/IEC 27001.

- **File access controls,** as to what types of staff and which specific staff are allowed to access specific files, are **managed through permissions** that are administered by our IT Manager. These permissions are individual specific, linked to users' IDs and managed by individual passwords.

- **Vulnerability Scans and Penetration Testing of our Internal Network** are scheduled to occur annually or when new hardware and/or Internet facing services are added to our network.

  These activities are undertaken by Comsmart, a New Zealand-owned IT solutions specialist.

Integration

Where a client's administrative data is required to be integrated with their survey data, we complete this using the information provided with the original sample received from the client rather than by requesting this information for only the achieved sample. To do the later would compromise the anonymity of respondents as required by the Codes of Practice of ESOMAR and RANZ.

The resulting file is then **depersonalised** before it is provided to the client. This is also a requirement under the Codes of Practice of ESOMAR and RANZ.

Data storage

All digital data is **stored indefinitely, in a depersonalised form**, which exceeds the minimum requirement of two years required by ESOMAR and RANZ. This is important in that it is not unusual for clients to re-contact us requiring data to be re-run for new projects they are working on. As outlined above, this does **not** include files of confidential customer information, which are usually deleted from our system or returned to the client by arrangement as required.

Data recovery and restoration

All files and all data are **continually being backed up**. Specifically, we run two types of backups; a real-time back up running in the background throughout business hours and a nightly backup.

Our real-time backup runs on our file server, allowing us to instantly restore a particular file at any stage during the current active backup day. All prior real-time daily back-ups are merged at the end of each business day to provide a single point of recovery. This backup stores up to three months of data onsite to allow for instant data restoration of our working files.

Importantly, this real-time backup not only runs and stores internally, it also runs and stores offsite – in an encrypted format – at a secure location (outside of Wellington City) as part of our Disaster Recovery Protocol.

The nightly backup not only backs up our files and data, it also backs up the servers themselves; both physical and virtual. This allows us, in combination with our real-time backup, to restore any server along with its files and data if a server was to fail.

Approach and measures to counter security attacks

Technically, we employ a managed Secure Internet Service providing Unified Threat Management (UTM) security features and functionality. Providing Firewall protection for both inbound and outbound connections to our network, this service also provides for AntiVirus and Spyware scanning, and Web URL and Content filtering.

Measures taken with the Firewall include those limiting the open ports to those that are required for business. As some of these ports are common ports, we also employ a Network Security Specialist to perform regular Intrusion Tests along with extensive logging to ensure we can prevent any external attempts at accessing our network.

Practically, what this means is that we have never (in the company's 25 year old history) lost the ability to provide our services due to any security issue.

Internally, we run a separate AntiVirus and AntiSpyware application on our desktops along with Mailmarshal for emails which itself utilises a third separate AntiVirus and AntiSpyware application.

We also have preventative measures in place in terms of connecting external media (e.g. usb drives), where alerts and automatic deletion of any suspicious files have been scanned.

Internal security requirements are met by security zones, virtual routers and VLANs. We then have policies with access control rules either allowing, denying or restricting access to certain security zones. These are continuously being inspected by UTM security features.

Support

We have a dedicated IT Manager who is responsible for maintaining the integrity of our IT infrastructure in general, as well as providing technical support to the call centre and our Survey Scripting Team.

Please also note that our IT infrastructure is state-of-the-art. It is constantly being monitored, regularly updated (OS, software and hardware updates) and as noted, backups are completed on a daily, weekly and monthly basis (i.e. real time).

Physical security

Our main office is located on Level 5 of the Bayleys Building in Brandon Street and our call centre on Level 4 of Midland Chambers, Johnston Street. That is, they are located in the same office block in the Wellington CBD.

Both the Bayleys Building and Midland Chambers are modern multi-storey buildings, with security able to be fully governed floor by floor by controlling lift access via a time-activated card security system. The stair wells are also controlled by this system. Staff are issued with personalised security cards, which enable their access to the main office to be monitored if necessary.

In addition, further security is provided in the following ways:

- Access to the reception area of our main office is electronically controlled, with visitors needing to ring on arrival at the door.
- Access to the call centre is controlled by a biometric system.
- Out-of-hours, the call centre is also monitored by an electronic security system and video camera surveillance.

Policy with regard to off-shore storage

Given our public sector client base, as a matter of policy, we do **not** store any files or data off-shore and do not intend to do so.

In fact, all client-provided files and data (e.g. samples of customers) are held on site (i.e. Midland Chambers) and are **not** at any stage stored in any other location where they are accessible. As noted above under *Data recovery and restoration processes*, backed up data is offsite, in an encrypted format, at a secure location (outside of Wellington City) as part of our Disaster Recovery Protocol.