Research New Zealand – Data Security Policy and Practice

Introduction

Given our Wellington-based location and our largely public sector client base, we have invested significantly in security software.

Technically, we use a Juniper Networks Firewall which is a purpose-built, modular VPN security platform. Protection is delivered by proven unified threat management (UTM) security features that are backed by best-in-class partners. We use the latest virus software (AntiVirus and AntiSpyware) which is automatically updated as new virus definitions are available.

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.

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.

Files containing confidential customer information

As an added layer of security, we have developed policies and practices to ensure that files received from and data repatriated to clients containing confidential information are not compromised.

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) are only accepted by us in an encrypted, password protected form, either on a memory stick, CD-Rom/DVD or through a secure client-only area of our website. We recommend our clients use the client-only area of our website to provide and receive confidential files.

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.

Access control

As noted above under *Introduction*, internal access to files 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.

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 Code of Practice of the Research Association of New Zealand Inc.

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 Code of Practice of the Research Association of New Zealand Inc.

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 tape drive 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 daily, weekly and monthly backups are performed on all servers. These backups are performed and stored on tapes and on our SAN. With the backup tapes being stored offsite, storing backup data on our SAN allows for instant access to recovery data going back seven days.

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 Code of Practice of the Research Association of New Zealand Inc.

The resulting file is then depersonalised before it is provided to the client. This is also a requirement under the Code of Practice of the Research Association of New Zealand Inc.

Approach and measures to counter security attacks

Onsite, we employ a Firewall to help protect our internal network from external security attacks. 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.

Internally, we run two separate AntiVirus and AntiSpyware applications on our desktops along with Mailmarshal for emails which itself utilises a third separate AntiVirus and AntiSpyware application. We provide web filtering and alerts to provide our users with advice on the safety of their web browsing.

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.

Physical security

All work is completed in our offices which are located on Level 7 (main office) and Level 4 (call centre), Resimac House, 45 Johnston Street, Wellington.

Resimac House is a modern multi-storey building in the CBD, with security able to be fully governed floor by floor by controlling lift access via a time-activated card security system. The stair well is also controlled by this system. Staff are issued with personalised cards, which enable their access to the main office to be monitored if necessary.

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

- On Level 7 (our main office), the reception area is separated from the main work area by self-shutting doors that are key-pad operated. Out-of-hours, the reception area is also monitored by an electronic security system.

- Access to the call centre on Level 4 is controlled by a biometric system. Out-of-hours, the call centre is also monitored by an electronic security system.

Data storage off-shore & in the 'cloud'

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 files and all data are held on site (i.e. Resimac House) and 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.

All survey data is stored indefinitely as required by the Research Association of New Zealand Inc. As outlined above, note that this does not include files of confidential administrative information provided by clients for the purposes of completing their research projects, which is usually deleted from our system or returned to the client as required.

Similarly, as a matter of policy, we do not store any files or data in the cloud and do not intend to do so.

Support

Finally, please note 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, made up of both Windows Server 2008 R2 and 2012 servers along with VMware ESXi Servers and a SAN. 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).