INFORMATION SECURITY QUESTIONS AND ANSWERS
Market Research Industry
This presentation provides an awareness of information security and its impact on the market research industry based on a risk assessment undertaken by the AMSRO Quality Committee.

This session comprises a series of Questions and Answers.

After presenting the Q & A’s, the forum will be open for additional questions.
Q 1: What is information Security about?

In general terms its about INFORMATION MANAGEMENT AND COMMUNICATION:

INFORMATION AND WHERE/HOW/BY WHOM THE INFORMATION IS MANAGED:

- Computers and their electronic content (digital data)
- Access to computers and data on computers and other electronic devices
- Paperwork – hard copy information
- People with access to computers and information (what they say and what they do).
Q 2: How do you classify information security risks across an organisation?

It's best classified according to the nature of risks:

1. ASSETS SECURITY RISK
2. PEOPLE SECURITY RISK
3. OPERATIONAL RISK
4. COMMUNICATIONS SECURITY RISK
Q 3: ASSETS: What are ASSET risks?

ASSETS are mostly the hardware and software used by the organisation but are also buildings and other data storage areas:

• COMPUTERS/OTHER DEVICES AND COMPUTER NETWORKS including cloud networks that store digital data. This includes access to computers and computer network.

• DATA stored on computers, other devices and computer network.

• BUILDINGS where computers and networks are held

• MOBILE ASSETS such as laptops, phones etc. are also assets
Q 4: ASSETS: What are the actual RISKS associated with assets?

- COMPUTERS – data loss through network and hardware failure, breach of systems and hardware infection
- HACKERS/MALWARE/VIRUS – infect computer software and hardware incl. mobile hardware
ANSWER ASSETS: What practical ASSET CONTROLS can be put in place?

- PASSWORD PROTECTION – stringent not ad hoc or ‘sloppy’
- Virus and malware protection software – test regimes for software including cloud technology usage
- DO NOT ALLOW STAFF TO UPLOAD SOFTWARE ONTO MOBILE DEVICES.
- Strict policies and protocols around the use of CDs, DVD or USB Drives, smart phones, laptops, iPads etc. – anything that could hold confidential data
ANSWER Cont: ASSETS: What practical ASSET CONTROLS can be put in place?

- **FIREWALL PROTECTION** i.e. hardware or software network device that forms a break between two networks to control the flow on information. One of the networks is usually the internet so it acts as a protective wall against intrusion.

- If staff have laptops that plug into the company network, there should be a firewall set up in place.

- **USE TIMEOUT SETTINGS** on laptops, say 5 minutes, after which a password is required to continue with access to information.
ANSWER Cont: ASSETS: What practical ASSET CONTROLS can be put in place?

- BUILDING SECURITY ACCESS CONTROLS
- CLEAN DESK POLICY
- T & Cs / Employment Agreements in place - employees and contractors to comply with asset controls
- SMART EMAIL USAGE POLICY: TRAIN STAFF to recognise the signs of a hidden (email) attack such as NEVER clicking on an email link in an email. Cut and past the URL into your browser, which should auto block any virus / hacker attack.
Q 5: PEOPLE: When does a person become an information security risk?

- PEOPLE are often referred to as ‘insider’ risks. Either employees or subcontractors/vendors, become a security risk when they, either knowingly or unknowingly through their own behavior, work in a way that creates a risk to information security.

Examples include; sharing passwords, talking about clients on face book and chat rooms, losing assets such as laptops etc.
Q 6: PEOPLE: Why are Vendors/Subcontractors a risk?

Vendors/Subcontractors often have as much or more access to company systems without the training or monitoring of their use. Often there is no exit strategy on contract completion.

Vendors/Subcontractors can also be people working from home such as recruiters, data analysts etc. Vendors can also be providers of cloud services, software developers and other like services.

Data is often communicated via email and rarely do companies check to ensure virus protection etc. is in place nor have a process to ensure data is securely removed from vendor assets post project.
ANSWER: PEOPLE : What practical controls can be put in place to minimise the risk?

Have strong HR Business systems in place that are implemented and monitored for compliance:

- Information Communications Policies - various
- Monitoring the appropriate use of company assets (smart phones & laptops etc.)
- Employment screening, entry and exit policies and employment agreements
- Disciplinary procedures for failure to follow protocols and processes
ANSWER Cont: PEOPLE: What practical controls can be put in place to minimise the risk?

- Tight inventory controls of assets such as laptops, smart phones of this employee group with ‘Acceptable Assets Use Policy’.
- Monitoring of the use to protect from uploading of unauthorised software etc.
- Periodic audits/checks of policies and procedures to ensure they are being enacted
ANSWER: VENDORS : What practical controls can be put in place to minimise the risk?

It depends on your business risks, for instance, if you work in the domain of clients involved in health or banking industries, you will require more controls because these industries demand it (& legislation demands it of them).

Examples of controls:

• Setting up levels of data classification SECURE LEVELS for high risk IS work to ensure only limited personnel have access and that access requires a two step authentication process.
ANSWER Cont: VENDORS : What practical controls can be put in place to minimise the risk?

- Contracts and/or service level agreements.
- Copies of vendor IS protocols and processes in place – if cloud services are provided, ensure appropriate risk controls are in place at least equal to your own controls.
- Get a copy of the breach notification process from vendors and ensure you are notified of any likely breach within 24 hours of occurrence

Internal audits and IT testing of access by vendors is also a useful tool.
Q 7: OPERATIONAL RISK: What are operational risks?

Market research operations include dealing with the confidentiality, security, integrity and availability of information. This includes preservation of data, checking authenticity, sending/receiving, sharing data and media handling (secure removal of data).

OPERATIONAL RISK is the protection of all of the above from malware (malicious software), ransom type software.
ANSWER: OPERATIONAL RISK: What practical controls can be put in place?

These are your typical IT risk controls:

- Malware protection software
- Firewalls
- Back ups of information, software and system images. Backups must be secure and free from virus risk
- Ditto to all of the above with vendors/subcontractors.
- Tight controls over installation of software applications (including apps).
ANSWER Cont: OPERATIONAL RISK: What practical controls can be put in place?

• Removal and disposal of media handling protocols tested to ensure secure data removal is really secure and the data has been removed. This especially applies to cloud services.

• Media transfer protocols protected against unauthorised access – test this protocol for effectiveness.
Q 8: COMMUNICATIONS SECURITY RISK: What are communications security risks?

Market research organisations receive and communicate information. This can be electronic media, hard copy (print form) or combination of both. Information security involves protecting the information from unauthorised person whilst still delivering the necessary content to the intended parties.

The risks are obvious:

- Failure to comply with the Privacy Principles and Code 2014.
- Failure to protect data during information transfer
- Network failure exposing data to unauthorised users
Q 8. COMMUNICATIONS SECURITY RISKS

Q 8 Cont: COMMUNICATIONS SECURITY RISK: What are communications security risks?

• No classification in place to determine authorized data security levels – anyone can see any document
• Paperwork not considered part of information security risk – multiple copies made without consideration to security of content. Often information sent electronically is printed by the recipient. If it is information sensitive and there is not policy in place to either mark it as secure data or control its use, then the hard copy becomes a risk.
RISK: What are the practical solutions?

These are a combination of IT solutions and people related processes:


• Confidentiality / non-disclosure agreements in place with stakeholders and audited for compliance.

• Strict protocols around use of social media on company asset.
COMMUNICATIONS SECURITY RISK: What are the practical solutions?

• IT security and confidential usage policies in place covering use of all information communication technology devices within the company?
• Above to be audited / tested for compliance.
• Network controls in place including segregations, firewalls, and other controls.
• Authorities and controls over generation of hard/ print copy material including confidential destruction.
ANSWER Cont: COMMUNICATIONS SECURITY RISK: What are the practical solutions?

- Mark information sensitive documents accordingly to warn the user.
- Restrict printing of documents to only certain hierarchies of documents.
- Have a clear desk policy for all information that is business sensitive.
- Ensure a procedure for hardcopy record keeping, archiving and secure destruction is in place.
Q 9: ARE WE BEING PARANOID?

It's only paranoia until a significant data breach occurs that impacts financially and legally on the company and has an on flow effect to the rest of the industry, then we were not paranoid enough.