INFORMATION TECHNOLOGY AND SECURITY RISK MANAGEMENT: TOP 12 RISKS

AUSTRALIAN DATA AND INSIGHTS ASSOCIATION

WHAT ARE THE RISKS? WHAT ARE THE SOLUTIONS?

Risks are numbered according to highest risk rating one to twelve.

Introduction

In dealing with the public and with any information entrusted to our care by them or for them, ADIA members should remember that our industry relies largely on their good will. When addressing the perceived risks in this guideline, therefore, members should always keep the best interests of the public in mind.

Based on the ISO 27001/2 Information Technology and Security Standards, the Top 12 Risks Guideline is an overview of an information security management system and identifies the main risk areas for research organisations and how they might impact on both internal and external operations.

The ADIA Quality Committee has identified the four following key risk review areas that can be undertaken in conjunction with ISO 20252 to help ensure your organisation mitigates Information Technology risk:

- **Communications**
- **Operations**
- **People** and
- **IT Assets Security**

The TOP 12 RISKS	Key Risk Review Area
#1 - Information Transfer	Communication Security
#2 - It Security Policies	Communication Security
#3– Protection from Malware	Operations Security
#4 - Network Security Management	Communication Security
#5 - User Responsibilities	People Security
#6 - People Prior to Employment or Contracting	Operations Security
#7 - People Termination/Change of Employment or Contract	Operations Security
#8 - Mobile Devices & Teleworking	IT Assets Security
#9 - System Backups	Operations Security
#10 - Control of Operational Software	Operations Security
#11 - Media Handling	Operations Security
#12 - Responsibility for Assets	IT Assets Security

INFORMATION TECHNOLOGY AND SECURITY RISK MANAGEMENT: TOP 12 RISKS

AUSTRALIAN DATA AND INSIGHTS ASSOCIATION

The 12 risks are grouped by their relevant key risk review area with solutions for managing each risk:

1. COMMUNICATION SECURITY

Communication securities are the measures and controls taken to deny unauthorised persons information derived from telecommunications whilst still delivering the necessary content to the intended recipients.

#1 RISK - INFORMATION TRANSFER

- What processes do you have in place to send and receive sensitive [i.e. client/respondent personal information, financial, commercial in confidence documentation, regulatory information etc.] data internally and externally?
- How secure are these processes – would they meet the Australian Privacy Principles? The Privacy (Market and Social Research) Code 2014? Have you ever tested them?
- Do you have formal confidentiality, non-disclosure agreements in place with staff and external stakeholders?
- What controls do you have in place for the use of electronic messaging such as email and twitter?

SOLUTIONS

1. **Information transfer policies** - Information transfer policies and procedures prescribing minimal mandatory controls in place to protect the transfer of information through the use of all types of communication facilities within the organisation.
2. **Agreements on information transfer** - Agreements between parties on information transfer shall address the secure transfer of business information between the organisation and any external party.
3. **Electronic messaging** - Information sent or received via information messaging processes shall have mandatory controls in place.
4. **Agreements** - Confidentiality or non-disclosure agreements with stakeholders need to be in place reflecting the organisations needs for the protection of information. These must be in a documented agreed format and periodically reviewed against legislation and any other need for change.

#2 RISK - IT SECURITY POLICIES

- Do you have IT security and confidential usage policies in place that cover the use of all Information Communication Technology devices within the company?
- How do you ensure policies are communicated internally and externally e.g. contractors?
- How do you know the policies are being adhered to? What procedures do you have in place to ensure compliance?

SOLUTIONS

1. **Information security policies** - Set of policies for information security shall be defined, approved by the Executive, published and communicated to employees, consultants/contractors and other relevant external parties [including clients].
2. **Review** - Policies shall be reviewed at planned periodic intervals or if a significant change occurs to ensure their continuing suitability, adequacy and effectiveness.

#4 RISK - NETWORK SECURITY MANAGEMENT

- How do you check your internal network to ensure there are no unintended users or access to the system? (An example could be security software running a test log and providing daily/periodic reports.)
- If you outsource network provisions, what service level agreements do you have in place that ensure network security management/checks are in place AND that you will be informed of any breeches of security?
- Are your networks segregated from one another by firewalls or other mechanisms so that any risk of malicious attack cannot spread from one to another network? An example could be your internal HR/ finance systems segregated from the client/project network. Another typical control could be to have highly sensitive/secure data on a network free from external interfaces such as internet access.

SOLUTIONS

1. **Network controls** - Networks shall have in place controls and be managed to provide sufficient protection of the information within the systems and applications.
2. **Security of network systems** - Security mechanisms, service levels and management requirements of all network services shall be identified and included in network service agreements, whether these services are provided in-house or outsourced.
3. **Segregation of networks** - Groups of information services, users and information systems shall be segregated on networks as a security measure.

2. OPERATIONS SECURITY

Operations securities are the systems and processes for the preservation of confidentiality, integrity and availability of information including properties such as authenticity, accountability, nonrepudiation [guarantees from sender/receiver of data] and reliability. End point security forms part of systematic operations security e.g. firewalls, antivirus software and intrusion detection for cloud software.

#3 RISK – PROTECTION FROM MALWARE

- Do you have software that protects all your IT devices from the introduction of malicious software (i.e. such as Crypto Locker virus which encrypts your computer content and locks down your computer until you pay a fee/ransom?)
- Do you have a policy in place that controls what software your employees can upload onto company electronic devices (including mobile phones, laptops, iPads etc.)?

SOLUTIONS

1. **Malware controls** - Detection, prevention and recovery controls are put in place to protect against malware. These controls must be implemented in conjunction with appropriate user awareness.

#9 RISK - SYSTEM BACKUPS

- How do you manage the process of backups of information, software and system images to ensure frequency and effective back up without risk of data loss or security breaches?

- Do you know whether the same standards apply to your subcontractors in relation to your secure information, particularly where subcontractors are operating cloud technology?

SOLUTIONS

1. **Information backup** - Back up copies of information, software and system images shall be taken and tested regularly in accordance with an agreed back up policy.

#10 RISK - CONTROL OF OPERATIONAL SOFTWARE

- What controls are in place in relation to installation of [approved corporate or unapproved private/contractor] software onto corporate systems including portable devices such as laptops etc.? (An example might include an employee's child uploading games onto portable devices, which present malware risks.)

SOLUTIONS

1. **Software installation** - Procedures in place including supervision and reporting for the installation of software on operational systems including portable devices.

#11 RISK - MEDIA HANDLING

- How do you manage the removal of secure data that may need archiving and re-instating later, OR alternatively, permanent removal so it can never be accessed or recovered again?
- Have you ever tested how stringent this process is? Is permanently removed data really never able to be recovered?
- What processes are in place to ensure permanent removal or destruction of media held within cloud services? Have they been integrity tested?
- What about your contractors? Are their processes as robust as your processes?

SOLUTIONS

1. **Management of removable media** - Procedures in place and implemented for the management of removable media.
2. **Disposal of media** - Media shall be disposed of securely when no longer required, using formal agreed procedures.
3. **Physical media transfer** - Media containing information shall be protected against unauthorised access, misuse of corruption during transportation.

3. PEOPLE SECURITY

#5 RISK - USER RESPONSIBILITIES

- Do you have IT security and confidential usage policies in place that cover the use of all electronic devices within the company?
- How do you ensure policies are communicated internally and externally e.g. contractors?
- How do you know the policies are being followed?

SOLUTIONS

1. **Secret authentication information** - Users shall be required to follow the organisations practices in the use of secret authentication information.
2. **Data storage devices** - Use of USB sticks (and the like) are controlled with secure data restrictions.

#6 RISK - PEOPLE PRIOR TO EMPLOYMENT OR CONTRACTING

- Do all your employees sign a confidentiality agreement and/or terms of conditions of employment? Is the agreement/employment conditions explained in plain language and periodically renewed?
- Do contractors/consultants sign a contract agreement incorporating confidentiality and IT security standards requirements?
- Do your contractors have appropriate liability insurance covering breaches of IT security and/or confidentiality requirements?
- Do you have a recruitment process in place that considers high level IT security access risks against each position description?

SOLUTIONS

1. **Screening** - Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, industry standards and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
2. **Terms and conditions of employment** -The contractual agreements with employees and contractors shall state their and the organisations responsibilities for information security.

#7 RISK - PEOPLE TERMINATION/CHANGE OF EMPLOYMENT OR CONTRACT

- Do you have a formal exit strategy that protects your interests once an employee has left the company or you terminate a formal agreement with a contractor? Does the exit strategy protect you from disclosure of information about your clients and other high risk by the exiting parties?
- Does your exist strategy ensure IT security is not compromised with passwords remaining on the system, mobile devices not returned or data disabled?

SOLUTIONS

1. **Termination or change of employment responsibilities** - Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee (or contractor) and enforced.

4. IT ASSETS SECURITY

#8 RISK - MOBILE DEVICES & TELEWORKING

- What mobile devices are used in your company that could pose a risk to your client, respondent or other secure data? What limitations have you put in place to control restrictions of secure data on mobile devices?
- Is data readily removed [or replicated] from your secure office to a home office or other external facilities such as, vehicles or contractor premises? What controls do you have in place to ensure data security is as tight elsewhere as it is in the office?

SOLUTIONS

1. Mobile device policy - A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.
2. Teleworking - A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.

#12 RISK - RESPONSIBILITY FOR ASSETS

- How do you manage the safe use of company assets including software licenses, laptops, notepads, iPads, smart phones etc. to ensure the rules of acceptable use protect the company from corruption of data, data security breaches and general misuse by unauthorised persons such as employees family?
- What rules apply to protect the business when the employee owns the asset?
- What happens to assets when employees leave the company? Remember assets include USB sticks, phones with client details and emails saved.

SOLUTIONS

1. Inventory of assets - Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.
2. Ownership of assets - Assets maintained in the inventory shall be owned [subject to risk control].
3. Acceptable use of assets - Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.
4. Return of assets - All employees and external party users shall return all of the organisational assets in their possession upon termination of their employment or contractual agreement.

For further information please contact:
The Australian Data and Insights Association
0460 012 092or email: admin@dataandinsights.com.au

AUSTRALIAN DATA AND INSIGHTS ASSOCIATION
TRUST MARK MEMBER
PRIVACY QUALITY ETHICS

For further information regarding the ISO 27001 Standard
please see - https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en