Information for agencies

Information Security Risk Statement Library

Risk statements

This document lists the risk statements published across all of OVIC’s information security incident notification insights reports.

| The risk of… | Caused by… | Resulting in…[[1]](#footnote-1) | |
| --- | --- | --- | --- |
| Unauthorised disclosure of personal information  ***(Compromise of confidentiality)*** | Employees accidentally sending emails to incorrect recipients | Impact to individuals whose personal information was affected | |
| Unauthorised collection and use of client information  ***(Compromise of confidentiality)*** | Former employee extracting data from a system for their own personal gain | Financial impact to the organisation | |
| Unauthorised handling of customer records  ***(Compromise of confidentiality)*** | Third party employees with inappropriate email settings | Impact to legal and regulatory compliance | |
| Unauthorised access to health information  ***(Compromise of the availability)*** | Malicious external threat actor intercepting mobile communications | Impact to service delivery | |
| Unauthorised modification of a database  ***(Compromise of the integrity)*** | Cybercriminal exploiting a vulnerability in a cloud hosted system | Impact to individuals whose personal information was affected | |
| Unauthorised access to government information  ***(Compromise of the confidentiality)*** | Inappropriate disposal of hard copy records | Impact to reputation | |
| Unauthorised disclosure of employee information  ***(Compromise of confidentiality)*** | Incorrect permissions set on shared drive / MS Teams / line of business system / Google drive | Impact to individuals whose personal information was affected | |
| Inappropriate handling of investigations information  ***(Compromise of confidentiality)*** | Employee using unauthorised third-party software not approved by the organisation | Impact on public services (reputation of, and confidence in, the organisation) |
| Inappropriate handling of identity information  ***(Compromise of confidentiality and integrity)*** | Employees failing to follow the identity checking process and being helpful to callers probing for information over the phone to change other customer records | Impact to individuals whose personal information was affected | |
| Loss of client files  ***(Compromise of availability)*** | Third party suffering a ransomware attack | Impact to service delivery | |
| Customers not receiving their documents (letters/bills) in a timely manner  ***(Compromise of availability)*** | Physical mail missing and not reaching intended mailing address | Impact to individuals | |
| Misuse of customer information for personal gain  ***(Compromise of confidentiality)*** | Employees looking up customers’ records without legitimate business reason | Impact to individuals whose personal information was affected  Impact on public services (reputation of, and confidence in, the organisation) | |
| Accidental access to client information  ***(Compromise of confidentiality)*** | Third parties not following the labelling requirements of the organisation | Impact to individuals whose personal information was affected | |
| Customers not receiving their letters in a timely manner  ***(Compromise of integrity and availability)*** | Employees not paying attention and inputting incorrect data into customer database | Impact to individuals whose personal information was affected | |
| Unauthorised access to systems and data  ***(Compromise of confidentiality and availability)*** | Malicious threat actors stealing government devices and poor password practices by employees (password stuck on stolen device) | Impact on service delivery  Impact on public services (reputation of, and confidence in, the organisation) | |
| Financial fraud  ***(Compromise of integrity)*** | | Malicious threat actors conducting a business email compromise (**BEC**) and intercepting communications | Impact on organisation’s finances |
| Unauthorised access to sensitive information after purchasing a second-hand computer  ***(Compromise of confidentiality)*** | | Authorised third-party not sanitising computers prior to reselling | Impact on public services (reputation of, and confidence in, the organisation)  Impact to individuals whose personal information was affected |
| Unauthorised access to hard copy documents containing personal information  ***(Compromise of confidentiality and availability)*** | | Threat actor accessing key-safe box mounted on the exterior of the building and gaining entry to steal assets | Impact to individuals whose personal information was affected  Impact on service delivery |
| Financial fraud  ***(Compromise of confidentiality and integrity)*** | | Internal staff intentionally accessing customer accounts and changing bank details | Impact on organisation’s finances  Impact to individuals whose personal information was affected |
| Unauthorised access to sensitive information  ***(Compromise of confidentiality)*** | | Malicious threat actor launching a cyber-attack on an authorised third-party who retained public sector information longer than the required timeframe | Impact on public services (reputation of, and confidence in, the organisation)  Impact to individuals whose personal information was affected |
| Unauthorised access to / inability to access public sector information  ***(Compromise of confidentiality and availability)*** | | Lost backup tapes during transit from authorised third party to public sector organisation | Impact to individuals whose personal information was affected  Impact on service delivery |
| Poor data quality  ***(Compromise of integrity)*** | | Internal staff manually processing an application and inadvertently linking it to the wrong case | Impact on public services (reputation of, and confidence in, the organisation)  Impact to individuals whose personal information was affected |
| Unauthorised access to / inability to access public sector information  ***(Compromise of confidentiality and availability)*** | | Thieves breaking into an authorised third-party premises and stealing a book / hard copy files and hard drive | Impact on service delivery  Impact on public services (reputation of, and confidence in, the organisation) |
| Unauthorised access to public sector information  ***(Compromise of confidentiality, integrity, and availability)*** | | Malicious threat actor hacking third-party application account credentials that are the same as credentials used on VPS systems to either access public sector systems or publish on dark web | Impact on public services (reputation of, and confidence in, the organisation)  Impact on service delivery  Impact to individuals whose personal information was affected |
| Employee payroll information shared without employee consent with a superannuation fund  ***(Compromise of confidentiality, integrity)*** | | System change triggering an override function and subsequently incorrectly processing data, reverting employees to the default fund and informing the fund | Impact on public services (reputation of, and confidence in, the organisation)  Impact to individuals whose personal information was affected |
| Inability to access public sector information  ***(Compromise of availability)*** | | System crash following a staff member rebooting one network device after a configuration change which caused a chain reaction on the rest of the network leading to connectivity issues | Impact on service delivery  Impact on public services (reputation of, and confidence in, the organisation) |
| Inadvertent release of client information  ***(Compromise of confidentiality)*** | | Public sector organisation not redacting documents | Impact on public services (reputation of, and confidence in, the organisation)  Impact to individuals whose personal information was affected |
| Inappropriate handling and disclosure of payment information  **(Compromise of confidentiality, integrity)** | | Storing unredacted credit card information | Impact on legal and regulatory compliance requirements e.g. payment card industry data security standards (**PCI-DSS**)  Impact to individuals whose personal information was affected |
| Inability to make phone calls or conduct electronic monitoring  **(Compromise of availability)** | | Telecommunications provider outage | Impact on service delivery  Impact on public services (reputation of, and confidence in, the organisation) |
| Unauthorised access to customer ticketing data  **(Compromise of confidentiality)** | | Malicious threat actor compromising fourth-party supply chain | Impact on public services (reputation of, and confidence in, the organisation)  Impact to individuals whose personal information was affected |
| Unauthorised disclosure of personal information or incorrect details due to utility bills being sent to incorrect recipient(s) and not the correct recipient  ***(Compromise of confidentiality, integrity and availability)*** | | System upgrade project with poor data quality | Impact to individuals whose personal information was affected  Impact to service delivery  Impact on public services (reputation of, and confidence in, the organisation) |
| Unauthorised disclosure of identity documentation  ***(Compromise of confidentiality)*** | | Accidental errors by internal staff not paying attention to detail or applying due diligence | Impact to individuals whose personal information was affected  Impact on public services (reputation of, and confidence in, the organisation) |
| Inability to access an online Workplace Health and Safety Management platform to undertake normal operational duties  ***(Compromise of availability)*** | | Reliance on authorised third party hosting the platform and being unavailable to answer/return any calls | Impact to service delivery  Impact on public services (reputation of, and confidence in, the organisation) |

1. The extent of the impact could be “limited” or higher depending on the context and nature of the incident and is left for an organisation to determine. [↑](#footnote-ref-1)