Data security

Over the last year, we've looked at how public organisations are using the data they hold to improve the services they provide to New Zealanders. We expect public organisations to have effective controls over information systems to prevent unauthorised access and loss or corruption of data. In this article, we summarise common data security themes from our audit work. Our focus was on the financial data that we audit.

By **data**, we mean forms of information held electronically by a public organisation. **Data security** is protecting that data from being lost or corrupted and from unauthorised access.

What are public organisations expected to do to protect their data?

Recent attacks on data security have increased the importance of getting the security of information systems right. Public organisations need to manage data security and privacy so that the data they collect is suitably protected, including when it's shared with other public organisations. When data security is breached, people can quickly lose trust and confidence in the public sector. It's important that public organisations respond to security issues in a proactive, rather than reactive, way.

New data security threats are constantly emerging. To stay effective, the controls over information systems must be regularly reviewed and updated.

Many of the recommendations we make during our annual audit work are about important cornerstones of good information system practice. Public organisations will be vulnerable to data security problems until they fix the basic weaknesses in security controls and procedures that we see during our audit work.

Recommendations about data security need to be implemented when they are made by internal or external specialists.

Who's responsible for data security?

Chief executives and senior leaders are accountable for managing risks in their organisation, including data security risks.

Managers put the controls in place, but the ultimate responsibility for data security sits with the most senior executive or the board, if there is one. Controls can be applied regardless of the size and complexity of the information systems. Control activities can be at a:

- **detailed process** level, to make sure the accounting records are reliable;

- **information system** level, ensuring that there is a defined information system strategy; or
- **governance** level, to support the public organisation's strategies and objectives.

Who helps public organisations with data security?

The Government Chief Privacy Officer and Protective Security Requirements support public organisations by making sure that appropriate information system controls are in place to minimise the risks identified by those charged with governance.

This approach is designed to result in a consistent approach throughout the public sector, and to support smaller organisations that may not have a large in-house IT team.

Not all public organisations are required to pay attention to guidance from the Government Chief Privacy Officer and not all have to meet the Protective Security Requirements. An organisation can choose to apply the guidance issued, even if they aren't required to do so.

The Government Chief Privacy Officer has issued core expectations that represent good practice for managing privacy. There's also a "Privacy Maturity Assessment Framework" to help public organisations assess their capability and make improvements. The Government Chief Privacy Officer has a long-term focus on privacy management and building privacy capability throughout the State service.

Public organisations need to manage data security and privacy so that the data they collect is suitably protected, including when it's shared

The Protective Security Requirements provide guidance on information security controls that could be implemented to reduce identified risks, and to help public organisations in determining the level of controls required. They're administered by the New Zealand Security Intelligence Service, on behalf of the New Zealand Intelligence Community.

Other sources of good practice include the *New Zealand Information Security Manual*, which provides guidance on information assurance and information systems security. Managed by the Government Communications Security Bureau, the manual also covers the security controls that are expected to be in place.

What's our role with data security?

The purpose of the annual audit is to obtain reasonable assurance that a public organisation's financial statements and performance information is materially correct.

During our annual audits, we usually review the information systems in the public organisation to the extent they are relevant to the preparation of the financial statements and performance information.

As part of our audit, we usually test a selection of controls relating to the security of financial data. Audit work is tailored to fit what the public organisation does, its size, and the complexity of its day-to-day business. We might test some controls on a rotational basis, such as at least once every three years. If a public organisation's controls are effective and working as intended, we'll do less detailed audit testing.

If significant controls aren't designed or implemented properly, or aren't working effectively, we tell the public organisation. Usually we do this through a recommendation made to those in charge – the most senior executive or the board, if there is one.

How did we identify common data security themes?

We reviewed the findings of our audits of 61 public organisations that are within the mandate of the Government Chief Privacy Officer and/or subject to the Protective Security Requirements. These public organisations complete privacy and protective security self-assessments. We'd expect the most senior executive or the board, if there is one, to be paying attention to these matters.

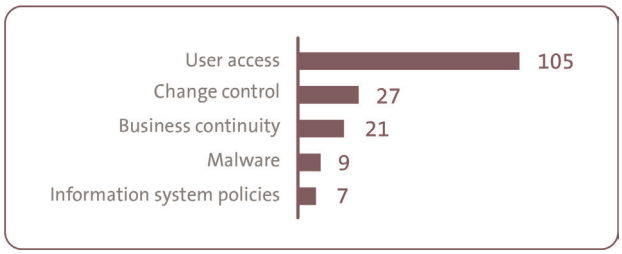
What common data security themes did we identify?

We made 742 recommendations in our reports to those organisations after the annual audits for the year ended 30 June 2017. Of those 742 recommendations, 169 were about data security

matters in the financial and performance information systems.

We put the 169 recommendations into five broad categories to help our analysis. Figure 1 shows how many recommendations were in each category.

Figure 1: Recommendations for the year ending 30 June 2017 relating to data security



We regularly identified basic weaknesses in security controls and procedures. Often, these were unresolved matters that we had identified already after previous audits. Several had been recurring for many years.

When responding to the recommendations, some public organisations did not appear to be resolving some of them as a matter of priority. This suggests that they considered the risks to be minor. We're not so sure. Here's a bit more about our findings for each category and why it's important that public organisations deal with these matters.

1 User access

Weak policies and procedures for user access increases the risk of unauthorised access to data.

Our findings included:

- staff and/or third-party contractors with inappropriate access to information system(s), including administrative and "superuser" accounts;
- former staff retaining access to information system(s);
- a lack of formal user-access reviews being performed or documented; and
- password policies that were weak or not enforced.

2 Change control

The procedures for making changes to masterfile data have to be robust. Unauthorised access could be used to change personal details of employees or supplier bank account details, increasing the risk of fraud.

Our findings included:

- no clear trail of changes made to the masterfile data;
- no clear trail or review of changes made to the information systems; and
- no clear trail of the user-testing strategy or retention of user-testing findings.

3 Business continuity

Public organisations need to have a disaster-recovery plan to minimise the amount of data that could be lost. That plan needs to include processes to recover data in the event of a data security breach.

Our findings included:

- back-ups not completed regularly or not in a separate secure location;
- no testing of back-ups to ensure that files can be restored;
- no formal review of system events and security logs; and
- no disaster management and recovery plan.

4 Malware

It is important that malware and firewall protection software is in place and up to date. If an information system's network security is easy to breach, the data held is vulnerable.

Our findings included:

- unnecessary delays in deploying security patches to servers and computers;
- security patches installed only in batches every six months; and
- information about installed patches wasn't recorded, except by the system on individual machines.

5 Information system policies

Policies need to be regularly reviewed to ensure that they reflect the changing technology environment and intent of the public organisation. Changes in the way public organisations store data, including moving to "cloud-based" services, can make current policies obsolete. This can result in employees failing to follow the principles of the policies and increase the risk of something going wrong.

Our findings included:

- no current information policies about security monitoring;
- policies that were not reviewed regularly; and
- no processes to ensure that third parties comply with the public organisation's information system policies.

What do our findings mean?

These findings aren't unique to the 61 public organisations that we focused on for this work. Instead, our auditors find these common themes throughout the public sector. They're also common in other countries – auditors in Australia have reported similar findings.

In our view, public organisations need to take these issues more seriously if data security risks are to be properly managed.

Questions arising from our work ...

If you're in charge of a public organisation, are you asking the following questions?

Do we manage user access to information systems appropriately?

Do we manage the changes made to information systems, including masterfile data, to ensure that all changes are authorised and understood?

Do we keep disaster recovery plans up to date and test them regularly to ensure that critical operations can be recovered quickly?

Do we implement timely security patches and service packs?

Do we regularly review information system policies to ensure that they reflect the changing technology environment and strengthen the governance of the public organisation?