Submission No 6

INQUIRY INTO CYBERSECURITY

Organisation: NSW Auditor General

Date Received: 8 September 2020

The Hon Tara Moriarty MLC
Chair, Portfolio Committee 1 – Premier and Finance
Parliament House
Macquarie Street
SYDNEY NSW 2000

Contact: Chris Clayton

Our ref: D2018586

8 September 2020

Dear Ms Moriarty

Inquiry into cybersecurity

Thank you for the invitation to make a submission to the Portfolio Committee 1 – Premier and Finance inquiry into cybersecurity. I welcome the Committee's examination of cybersecurity in New South Wales.

The effective management of cybersecurity risks has been and will continue to be an important focus area for my audit program. Recent audit reports addressing agencies' management of cybersecurity risks include:

- Universities 2019 financial audits published 4 June 2020
- Integrity of data in the Births, Deaths and Marriages Register performance audit published 7 April 2020
- Report on Local Government 2019 published 5 March 2020
- Report on Internal Controls and Governance 2019 published 5 November 2019
- Detecting and responding to cyber security incidents performance audit published 2 March 2018.

Relevant extracts from these reports are enclosed with this letter.

I have two further performance audits that I am conducting:

- **Managing cyber risks**[1]

  Following our 2018 audit of detecting and responding to cyber security incidents, this audit will examine how effectively agencies identify and manage their cyber security risks. This will include consideration of their compliance with the NSW Cyber Security Policy that came into effect in February 2019.

- **Service NSW's handling of personal information**[2]

  This audit will assess how effectively Service NSW handles personal customer and business information to ensure its privacy. This will include consideration of whether Service NSW has implemented policies, processes, systems and governance to identify and manage risks to the privacy of personal customer and business information, and to support the effective handling of personal customer and business information.

[1] https://www.audit.nsw.gov.au/our-work/reports/managing-cyber-risks
[2] https://www.audit.nsw.gov.au/our-work/reports/service-nsws-handling-of-personal-information

This audit is being conducted in response to a request from the Hon. Victor Dominello, Minister for Customer Service, under section 27B(3)(c) of the *Public Finance and Audit Act 1983*.

I continue to give focus to cybersecurity in my three-year forward program of audits. My annual work program, available at https://www.audit.nsw.gov.au/annual-work-program-2020-21, outlines the following topics related to cybersecurity.

Financial audit focus areas in response to recent emergencies – 2020-21

Financial audits will have regard to the bushfire and flood emergency and COVID-19, and the consequence that a significant number of remotely connected employees for an extended period may strain an entity's IT infrastructure and control environment. Our financial audits will address, amongst other things, accessibility to technology and the maturity of information technology systems and controls to prevent unauthorised and fraudulent access to data.

Compliance review: Cybersecurity – planned audit for 2020-21

In February 2019 the Department of Finance, Services and Innovation launched the NSW Cybersecurity Policy to ensure all NSW Government Departments and Public Service Agencies are managing cybersecurity risks to their information and systems. The policy mandates a number of requirements that are a minimum that all agencies must implement. In addition agencies must assess their level of cyber maturity. This audit will examine whether agencies are complying with the NSW Cybersecurity Policy.

Cybersecurity (State sector) – planned audit for 2021-22 to 2022-23

The Audit Office aims to conduct a performance audit on cybersecurity every two years in a selection of agencies. Our focus areas for this performance audit will be informed by our analysis of emerging risks and issues, and relevant findings in our financial audit volumes.

Cybersecurity (Local Government sector) – planned audit for 2021-22 to 2022-23

The increasing global interconnectivity between computer networks has dramatically increased the risk of cybersecurity incidents. Such incidents can harm local government service delivery and may include the theft of information, denial of access to critical technology, or even the hijacking of systems for profit or malicious intent. This audit will consider how well selected councils ensure they have effective cybersecurity measures in place.

Security and privacy of patient information – planned audit for 2020-21

Local Health Districts manage large volumes of private patient information and have their own systems for data management with differing approaches to data protection. Clinicians in busy hospital environments require timely access to data and systems to effectively treat patients. Increased accessibility may in turn increase the risk of poor data and system security practices. Recent experience in other jurisdictions has also demonstrated that operational assets that are controlled using technology may be a target for cyber-attacks. This audit could assess how effectively NSW Health is ensuring the privacy and security of patient data.

Security of student information – planned audit for 2020-21

Schools collect and maintain detailed student data, including sensitive personal information. Schools can also require or encourage students to use third party software applications for learning and other school related activities. This audit will examine how effectively schools ensure student data is secure – both within their own systems and when provided to third parties. This audit may also examine the effectiveness of information security governance as teachers and students moved to online learning in response to COVID-19.

Integrity of data in the land titles registry – planned audit for 2021-22 to 2022-23

Australian Registry Investments (trading as NSW Land Registry Services) was granted the right to operate the titling and registry operations of New South Wales in April 2017, under a 35-year concession which commenced on 1 July 2017.

The NSW Government continues to guarantee title under the Torrens Assurance Fund (TAF). The Office of the Registrar General regulates NSW LRS as the operator of the NSW land titles registry under a regulator operator model. This audit could examine how effectively the Registrar General monitors NSW LRS's operation of the land titles registry in respect of defined service levels, KPIs and the integrity and security of the data in the register.

I have recently received a number of requests for audits from Members of the Parliament of New South Wales relating to cybersecurity. These requests have been considered in developing my annual work program and the possible scope of the audits included on the work program. These requests for audit from Members of Parliament, and my response, are available on the Audit Office's website at https://www.audit.nsw.gov.au/our-work/requests-for-audit.

Thank you once again for the invitation to make a submission to the Committee's inquiry. Please don't hesitate to contact me if you would like further information about my reports to Parliament.

Yours sincerely

Margaret Crawford

Auditor-General for New South Wales

Encl.

Relevant extracts of recent audit reports to Parliament related to cybersecurity

Universities 2019 financial audits[3] – published 4 June 2020

3.2 Information technology

Cyber security

Cyber threats are becoming increasingly common and sophisticated as the global interconnectivity between computer networks has increased.

Cyber security comprises technologies, processes and controls that are designed to protect IT systems and sensitive data from cyber attacks. The cyber security framework consists of threat identification, protection, detection, response and recovery of IT systems.

Cyber incidents can harm universities' service delivery and may involve:

- theft of information such as intellectual property or sensitive personal data
- denial of access to critical technology
- hijacking of systems for profit or malicious intent
- financial losses.

Two NSW universities have not yet implemented a cyber risk policy

Recommendation (repeat)

NSW universities should strengthen cyber security frameworks and controls to protect sensitive data and prevent financial and reputational losses.

The trend in adoption of common cyber security controls at NSW universities is detailed below.

Cyber security control	Number of universities in 2019	Number of universities in 2018	Trend
Implemented a cyber risk policy	8	8	⊖
Maintained a cyber incidents register	9	7	⌃
Assessed the potential financial and/or operational impact of cyber attacks	8	7	⌃
Established a recovery plan following a cyber attack	10	8	⌃
Staff are formally trained in cyber awareness	7	6	⌃
Tested cyber resilience during the past year	6	5	⌃

Source: Provided by universities (unaudited).

The number of cyber incidents recorded in 2019 by the seven universities ranged from two to 982.

The disparity in the number of recorded incidents is because:

- there are different definitions of what a 'cyber incident' is
- some registers include intercepted or blocked attempts, while others do not.

[3] https://www.audit.nsw.gov.au/our-work/reports/universities-2019-audits

On average, universities incurred $4.6 million in costs in managing cyber security in 2019 ($4.0 million in 2018).

The Australian Cyber Security Centre (ACSC) has published mitigation strategies and recommended controls for protecting against cyber threats. This set of controls is referred to as the 'Essential Eight'. Some of these controls are not expensive to implement, yet provide important protections. Whilst universities are not required to adopt these controls, some aspects of the Essential Eight have been implemented at some NSW universities.

ACSC Essential Eight mitigation strategies	Number of universities that apply
1. Application whitelisting All non-approved applications (including malicious code) are prevented from executing.	5
2. Check and apply security patches Security vulnerabilities in applications can be used to execute malicious code on systems.	8
3. Configure Microsoft Office macro settings Microsoft Office macros can be used to deliver and execute malicious code on systems.	5
4. User application hardening Flash, ads and Java are popular ways to deliver and execute malicious code on systems.	3
5. Restrict / review administrative privileges Administrative user accounts have extensive access to systems and may be compromised.	9
6. Patch operating systems Security vulnerabilities in operating systems can be used to further the compromise of systems.	10
7. Multifactor authentication Stronger user authentication makes it harder for external parties to access sensitive information and systems.	9
8. Daily backups and test for restoration Ensure information can be accessed again following a cyber security incident.	10

Source: Provided by universities (unaudited).

Our 2018 performance audit report on Detecting and Responding to Cyber Security Incidents includes several findings that may be useful for universities to enhance their controls around cyber security risks.

Integrity of data in the Births, Deaths and Marriages Register performance audit[4] – published 7 April 2020

The NSW Registry of Births Deaths and Marriages (BD&M) is responsible for maintaining registers of births, deaths and marriages in New South Wales. BD&M is also responsible for registering adoptions, changes of name, changes of sex and relationships. These records are collectively referred to as 'the Register'. The *Births, Deaths and Marriages Registration Act 1995* (the BD&M Act) makes the Registrar (the head of BD&M) responsible for maintaining the integrity of the Register and preventing fraud associated with the Register. Maintaining the integrity of the information held in the Register is important as it is used to confirm people's identity. Unauthorised access to, or misuse of the information in the Register can lead to fraud or identity theft. For these reasons it is important that there are sufficient controls in place to protect the information.

BD&M staff access, add to and amend the Register through the LifeLink application. While BD&M is part of the Department of Customer Service, the Department of Communities and Justice (DCJ) manages the databases that contain the Register and sit behind LifeLink and is responsible for the security of these databases.

This audit assessed whether BD&M has effective controls in place to ensure the integrity of data in the Births, Deaths and Marriages Register, and to prevent unauthorised access and misuse. It addressed the following:

- Are relevant process and IT controls in place and effective to ensure the integrity of data in the Register and the authenticity of records and documents?
- Are security controls in place and effective to prevent unauthorised access to, and modification of, data in the Register?

Conclusion

BD&M has processes and controls in place to ensure that the information entered in the Register is accurate and that amendments to the Register are validated. BD&M also has controls in place to prevent and detect unauthorised access to, and activity in the Register. However, there are significant gaps in these controls. Addressing these gaps is necessary to ensure the integrity of the information in the Register.

BD&M has detailed procedures for all registrations and amendments to the Register, which include processes for entering, assessing and checking the validity and adequacy of source documents. Where BD&M staff have directly input all the data and for amendments to the Register, a second person is required to check all information that has been input before an event can be registered or an amendment can be made. BD&M carries out regular internal audits of all registration processes to check whether procedures are being followed and to address non-compliance where required.

BD&M authorises access to the Register and carries out regular access reviews to ensure that users are current and have the appropriate level of access. There are audit trails of all user activity, but BD&M does not routinely monitor these. At the time of the audit, BD&M also did not monitor activity by privileged users who could make unauthorised changes to the Register. Not monitoring this activity created a risk that unauthorised activity in the Register would not be detected.

BD&M has no direct oversight of the database environment which houses the Register and relies on DCJ's management of a third-party vendor to provide the assurance it needs over database security. The vendor operates an Information Security Management System that complies with international standards, but neither BD&M nor DCJ has undertaken independent assurance of the effectiveness of the vendor's IT controls.

[4] https://www.audit.nsw.gov.au/our-work/reports/integrity-of-data-in-the-births-deaths-and-marriages-register

Key findings

BD&M has processes in place to ensure that the information entered in the Register is accurate and that amendments to the Register are validated

BD&M has detailed procedures for all registrations which include processes for entering, assessing and checking the validity and adequacy of source documents. Where BD&M staff have directly input all the data, LifeLink requires a second staff member to approve the registration before it is entered on the Register. BD&M also requires documentation from two separate sources for birth and death registrations.

BD&M validates and authorises all requests for amendments to the Register and there is segregation of duties to ensure that the same officer cannot both create and apply an amendment. BD&M carries out regular internal audits of all registration processes to check whether procedures are being followed and to identify and address non-compliance.

BD&M authorises access to the Register and regularly reviews this access

BD&M has processes in place to authorise internal and third-party access to the Register, including Service NSW call centre staff and users who submit information via eRegistry. This authorisation process ensures that users are provided with the appropriate level of access. BD&M carry out regular user access reviews to ensure that the list of users is current and that users have the appropriate levels of access.

There are insufficient controls to prevent the distribution of information in the Register

There are currently insufficient restrictions placed on the ability of staff to export and distribute information from LifeLink. This increases the risk of unauthorised access to, and misuse of LifeLink data and creates the risk that information may be sent to unauthorised third parties.

Four staff members of BD&M can use specialised software to generate reports of data from the Register as part of their role in BD&M. There is an audit trail of this activity but at the time of the audit, BD&M was not reviewing this. BD&M has since commenced routine audits to address this.

BD&M does not actively monitor user activity in the Register

BD&M maintains audit trails of all activity in the Register but does not routinely monitor these to identify unusual activity or fraud by users including activity by Service NSW staff who have read-only access to the Register. At the time of this audit, BD&M also did not monitor audit trails of privileged user activity in the Register, but it has now commenced routine audits to address this. It is particularly important to monitor activity by privileged users because they have access to amend records and can enable unauthorised access to the Register.

BD&M does not have sufficient assurance over the effectiveness of database security controls

BD&M has no direct oversight of the database environment and relies on DCJ's management of a third-party vendor to provide the assurance it needs over database security. The vendor operates an Information Security Management System that is certified against international standards, but neither BD&M nor DCJ has undertaken independent assurance of the effectiveness of the vendor's general IT controls.

There are gaps in controls to prevent and detect unauthorised access to the databases and servers

Neither BD&M nor DCJ is regularly reviewing users who have access to the databases and related servers that sit behind the Register. They are also not monitoring user activity in these databases and servers. Passwords that individuals use to access the databases and servers are not configured in line with DCJ's policy on required password settings. This creates the risk of unauthorised access or changes to the Register that are not identified.

Recommendations

As a matter of urgency, the Department of Customer Service should ensure that the Registry of Births Deaths and Marriages:

1. works with the Department of Communities and Justice to ensure that passwords for users authorised to access the databases and servers comply with the Department of Communities and Justice's policy on password settings.

By July 2020, the Department of Customer Service should ensure that the Registry of Births Deaths and Marriages:

2. routinely monitors:
    - privileged user activity in the Register
    - other user activity in the Register including activity outside normal office hours
    - reporting software user activity.
3. restricts the ability of LifeLink users to export and distribute information from the Register outside of legitimate actions required for their role
4. updates the Service Partnership Agreement with Service NSW to include monitoring of Service NSW staff activity in the Register
5. performs regular fraud detection audits for eRegistry users
6. works with the Department of Communities and Justice to ensure that:
    - there are regular access reviews of users of the databases and servers that sit behind the Register
    - there is regular monitoring of activity of users who have access to the databases and servers that sit behind the Register
    - there are regular audits to provide independent assurance that database security controls operate effectively.
7. clarifies and formalises responsibilities with the Department of Communities and Justice in relation to the management of database security

By December 2020, the Department of Customer Service should ensure that the Registry of Births Deaths and Marriages:

8. undertakes a risk-based analysis of the impact of gaps in the controls to prevent unauthorised user activity on the historical integrity of data in the Register
9. implements remediating action stemming from recommendation eight.

Report on Local Government 2019[5] – published 5 March 2020

4.4 Cyber security management

Council's response to cyber security risks can improve

At a State Government level, the NSW Cyber Security Policy states that 'strong cyber security is an important component of the NSW Digital Government Strategy. The term cyber security covers all measures used to protect systems and information processed, stored or communicated on these systems from compromise of confidentiality, integrity and availability'. While there is currently no requirement for councils to comply with the State Government's cyber security policy, councils may find it useful to refer to the policy for further guidance.

Recommendation

The Office of Local Government within the Department of Planning, Industry and Environment should develop a cyber security policy by 30 June 2021 to ensure a consistent response to cyber security risks across councils.

Poor management of cyber security can expose councils to a broad range of risks, including financial loss, reputational damage and data breaches. The potential impacts may include:

- theft of corporate and financial information and intellectual property
- theft of money
- denial of service
- destruction of data
- costs of repairing affected systems, networks and devices
- legal fees and/or legal action from losses arising from denial-of-service attacks causing system downtime in critical systems
- third-party losses when personal information stored on government systems is used for criminal purposes.

We performed a high-level assessment to determine whether councils have the basic governance and internal controls to manage cyber security.

80% of councils do not have formal cyber security policy/framework

46% of councils have not included risk of cyber-attack in their risk register

67% of councils have not recently performed penetrations testing (cyber-attack simulation)

76% of councils have not delivered cyber security training to all of their staffs

84% of councils do not have separate cyber security budget

48% of councils do not have cyber security insurance policy

78% of councils do not maintain a centralised register of cyber incident

Councils' cyber security management requires improvement, as most councils are yet to implement the basic elements of governance, such as a cyber security policy or framework. This will continue to be an area of focus, with an upcoming performance audit planned on cyber security post 30 June 2020.

[5] https://www.audit.nsw.gov.au/our-work/reports/report-on-local-government-2019

Report on Internal Controls and Governance 2019[6] – published 5 November 2019

7. Managing sensitive data

This chapter outlines our audit observations, conclusions and recommendations, arising from our review of governance and processes in relation to the management of sensitive data.

Key conclusions and sector wide learnings

Information technology risks are rapidly increasing. More interfaces between agencies and greater connectivity means the amounts of data agencies generate, access, store and share continue to increase. Some of this information is sensitive information, which is protected by the *Privacy Act 1988*.

It is important that agencies understand what sensitive data they hold, the risks associated with the inadvertent release of this information and how they are mitigating those risks. We found that agencies need to continue to identify and record their sensitive data, as well as expand the methods they use to identify sensitive data. This includes data held in unstructured repositories, such as network shared drives and by agency service providers.

Eighty-eight per cent of agencies have established policies to respond to potential data breaches when they are identified and 70 per cent of agencies maintain a register to record key information in relation to identified data breach incidents.

Key areas where agencies can improve their management of sensitive data include:

- identifying sensitive data, based on a comprehensive and structured process and maintaining an inventory of the data
- assessing the criticality and sensitivity of the data so that the protection of high risk data can be prioritised
- developing comprehensive data breach management policies to ensure data breaches are appropriately managed
- maintaining a data breach incident register to record key information in relation to identified data breaches incidents, including the estimated cost of the breach
- providing on-going training and awareness activities to employees in relation to sensitive data and managing data breaches.

7.1 Background

The Information Management Framework outlines the shared direction of information management within the NSW Public Sector. The framework outlines the key elements of data management including identifying core information assets and systems and performing risk assessments of the high value information systems and assets an agency holds.

Good data management helps agencies deal with, and limit the impact of cyber attacks and other unauthorised access to the systems that hold that data. All agencies hold and manage sensitive data as part of their operations. Sensitive information includes employee personal details, credit information, medical records, patient personal details, drivers licence information, criminal records, young offenders' records, biometric information and other personal details. The management of risks associated with the inadvertent release of sensitive information is crucial to agency operations.

The loss of sensitive data can result in:

- fraudulent use of an individual's personal data
- financial loss to the agency and the individuals affected
- reputational damage and loss of public trust in the agency responsible for its safekeeping.

[6] https://www.audit.nsw.gov.au/our-work/reports/internal-controls-and-governance-2019

This chapter focusses on what agencies have done to identify and assess their sensitive data and to manage data breaches.

Risks posed by sensitive data can be easily overlooked or not identified

It is important for government agencies to know what sensitive data is, and how it is being controlled. Agencies should ask:

- How does sensitive data enter the agency?
- Where does it reside?
- How, and under what circumstances does it leave the agency?

These are simple questions, but without this understanding the risks posed by sensitive data can be easily overlooked or not identified. Our audits are focussed on agencies' key financial systems and not necessarily those systems that store sensitive personal data. However, over the years we have identified and reported gaps in relation to managing sensitive data. The examples below, as well as a multitude of highly publicised cases demonstrate how simple it can be for an agency to be exposed to data breaches, particularly if they are not assessing and actively managing the risks that arise from holding sensitive data.

Test databases

Unencrypted sensitive business data was copied to development and test environments where the information could have been copied on to USB devices. Various users had access to this data, including contracted developers.

Printers

Policies or procedures were not in place to cover the erasure of data on common printers accessed by external parties for support or repairs.

Access restrictions

A large number of database administrators at the agency and their service provider had access to modify and extract unencrypted sensitive data, without activity audit logging controls in place.

Data migrations

The security risks posed by a data migration project were not adequately managed. For example, there was:

- no policy of framework in place that dealt with user access security, data governance and physical and network security
- no risk assessment performed over the sensitive data to identify data masking requirements during migration and user acceptance testing
- no restrictions or process to ensure secure disposal of data and removal of user access from the migration environment.

Backups

Daily system backups of employee records were saved to a network drive in clear text format.

Exhibit 6: Examples of gaps identified in relation to managing sensitive data

Source: Audit Office management letters (2017 to 2019).

7.2 Identifying and assessing sensitive data

We reviewed the adequacy of agency processes to identify sensitive data and assess its risk.

Agencies are not proactively identifying sensitive data held and where it resides

An agency's ability to appropriately protect sensitive data is limited without a comprehensive understanding of all sensitive data held and where it is stored. Sixty-eight per cent of agencies maintain an inventory of their sensitive data. However, this may not be a complete inventory because, of these agencies:

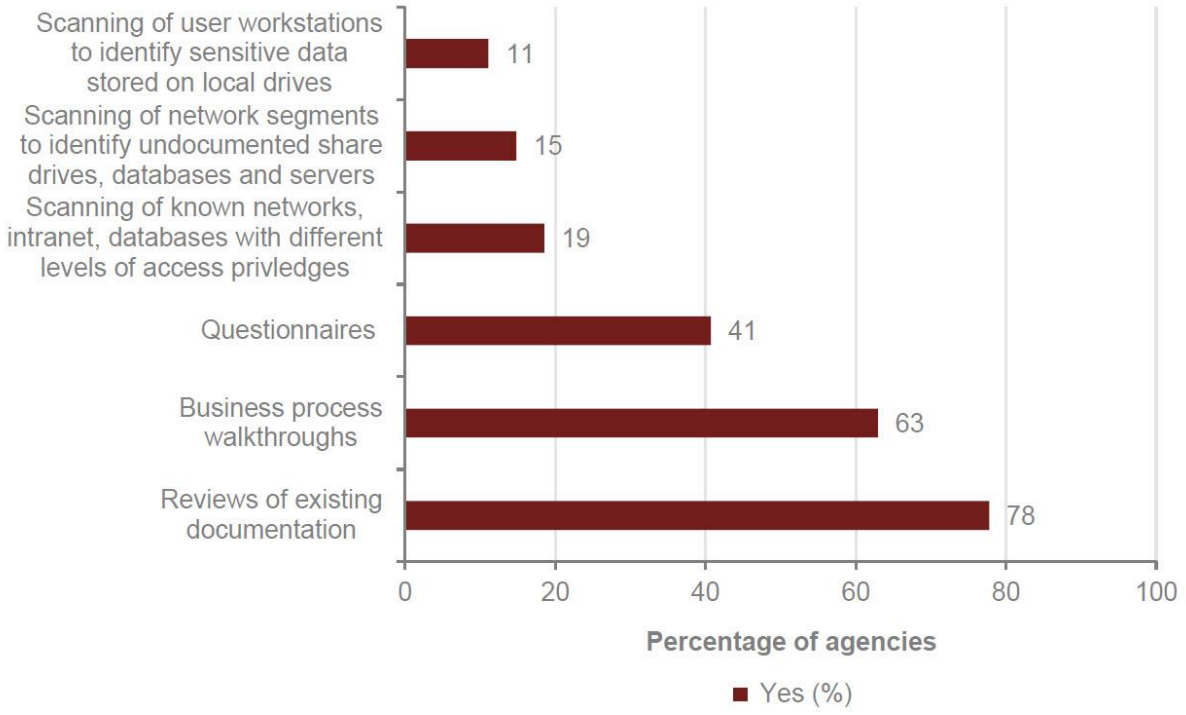
- 11 per cent had not captured data held in unstructured data repositories, such as shared network drives and email servers
- 29 per cent of agencies had not considered data held by their service providers.

We also found that the process whereby agencies identified their sensitive data was not always comprehensive. Generally, agencies relied on common processes such as reviewing existing documentation (e.g. data flow diagrams) and business process walkthroughs to identify sensitive data. Other processes were less commonly used, such as:

- using questionnaires sent to key officers, such as business process owners and database administrators
- scanning network shared drives, intranet sites and databases
- scanning network segments to identify undocumented shared drives, databases and servers
- scanning user workstations to identify sensitive data stored on local drives.

The use of common processes to identify where sensitive data is held increases the risk that not all sensitive data will be identified, meaning it may not be adequately protected.

The graph below shows the processes used by agencies to identify where their sensitive data is located within their IT infrastructure.



Identification processes for the location of sensitive data (of the 68% of agencies that had conducted an exercise)

Source: Audit Office analysis.

Agency processes to identify whether data is sensitive needs to improve

Only 74 per cent of the agencies performed a risk assessment as part of their sensitive data identification process to determine the data's criticality and sensitivity. Of these agencies, only 81 per cent had performed another level of review to assess the potential impact of the data loss to the agency. For example, impact assessments should consider:

- regulatory implications
- extent of financial impact
- level of business disruption
- magnitude of reputational damage.

Without a comprehensive risk assessment, data sensitivity may be inappropriately classified and resources may not be allocated to the highest risk data. Risk assessment procedures enable agencies to identify their high-risk data and prioritise its protection.

Not all agencies have developed data classification and labelling policies or guidelines

Eighty-five per cent of the agencies have established data classification policies or guidelines to define the classification of data. Inconsistent methods of classification and labelling increase the risk that sensitive information will be mishandled and not adequately protected.

The NSW Government Information Classification, Labelling and Handling Guidelines helps agencies identify the confidentiality requirements of information assets and apply suitable protective markings.

7.3 Managing data breaches

We reviewed the adequacy of agency policies and processes to adequately respond to data breaches.

Most agencies have developed a data breach management policy

Eighty-eight per cent of agencies have established policies to ensure all employees are aware of their roles and responsibilities when a potential data breach is identified. However, 14 per cent of agencies have not reviewed their data breach management policies by the scheduled date and, as noted in the table below, opportunities exist to make agency policies more comprehensive.

Maintaining up-to-date policies ensures all potential data breaches are appropriately managed by agencies and their staff and service providers. Without adequate guidance there is an increased risk data breaches go unreported and are not effectively managed. In addition, appropriate strategies would not be developed to prevent the reoccurrence of similar breaches in the future.

The table below highlights elements of agency data breach management and the percentage of agencies that include those elements in their policies.

Key elements of an agency data breach management (of the 88% of agencies with policies to manage data breaches)	Percentage of agencies (%)
Detailed approach (step by step) of how the agency will respond to a data breach incident	94
Instructions of the first response on how to contain the data breach	94
A process to evaluate a data breach is set out	94
Processes for how the agency will assess the root cause of the incident and plan any prevent future breaches	94
Guidance on how the agency will assess the risk associated with the incident	91
Detail on roles, responsibilities and accountabilities for handling data breaches	89
Notification procedures to inform internal and external stakeholders	80
Requirements on what, when and how to report data breaches and how they have been handled to those charged with governance	57

Source: Audit Office analysis.

Not all agencies maintain a data breach/incident register or measure the cost of data breaches

Seventy per cent of agencies maintain a register to record key information in relation to identified data breach incidents. This enables agencies to assess the circumstances and impact of the breach, and implement appropriate remedial actions. However, registers did not always contain all key fields, as set out in the table below.

The absence of a data breach register makes it difficult to determine whether the actions taken regarding the containment, evaluation and remediation actions of each data breach were appropriate. A register also enables agencies to develop effective preventative strategies, based on the type and seriousness of the breach.

The table below outlines better practice elements of data breach registers and the percentage of agencies whose registers contain those elements.

Key fields in data breach registers (of the 70% of agencies that maintain registers)	Percentage of agencies (%)
Date of incident	100
Description/nature of incident	100
Description of how the incident was contained	75
Details of how the data breach was evaluated	68
Details of assessment of the risk from data breach	61
Details of notified related parties and authorities	54
Details of applied preventative controls for future events	50
Estimated cost of data breach*	11

* While 11 per cent of agencies include this field in their incident register, none have recorded the cost of any recorded data breaches.

Source: Audit Office analysis.

As at 31 March 2019, agencies had recorded 3,324 data incidents, while no costs were recorded against these incidents. Although, we would expect agency investment decisions in data breach prevention and detection to be based on broader considerations, such as reputational and legal obligations, the cost of data breaches can be a relevant input in determining if investment is adequate. The exhibit below provides an indication of the cost of data breaches and significant steps required to resolve it.

The report highlighted that the cost of data breaches continues to increase, and more consumer records are being lost or stolen, year after year. The report estimated an average cost of:

- $148 per lost or stolen record
- $3.86 million per data breach.

The methodology applied in the report to estimate the cost to resolve data breaches was categorised into the following categories:

Detection and escalation

Activities to enable the detection and reporting of breaches to appropriate personnel within an appropriate timeframe. This includes:

- forensic and investigation activities
- assessment and audit activities
- crisis team management
- communication to the executive management and board of directors.

Notification

Activities to notify individuals who had data compromised in the breach as regulatory activities and communications. This includes:

- emails, letters, outbound telephone calls or general notice that personal information was lost or stolen
- communication with regulators, determination of all regulatory requirements and engagement of external experts.

Post data breach response

This relates to processes to assist affected individuals and customers of the data breach as well as costs associated to compensate the affected individuals and regulatory implications. This includes:

- help desk activities and inbound communications
- legal expenditures
- regulatory fines
- product discounts.

Lost business costs

These costs are associated with the cost of lost business such as business disruption, system downtime and customer churn. This includes:

- cost of business disruption and revenue loss during system downtime
- cost of lost customers and acquiring new customers
- reputation losses.

Exhibit 7: 2018 Cost of Data Breach Study: Global Overview issued by IBM Security and Ponemon Institute

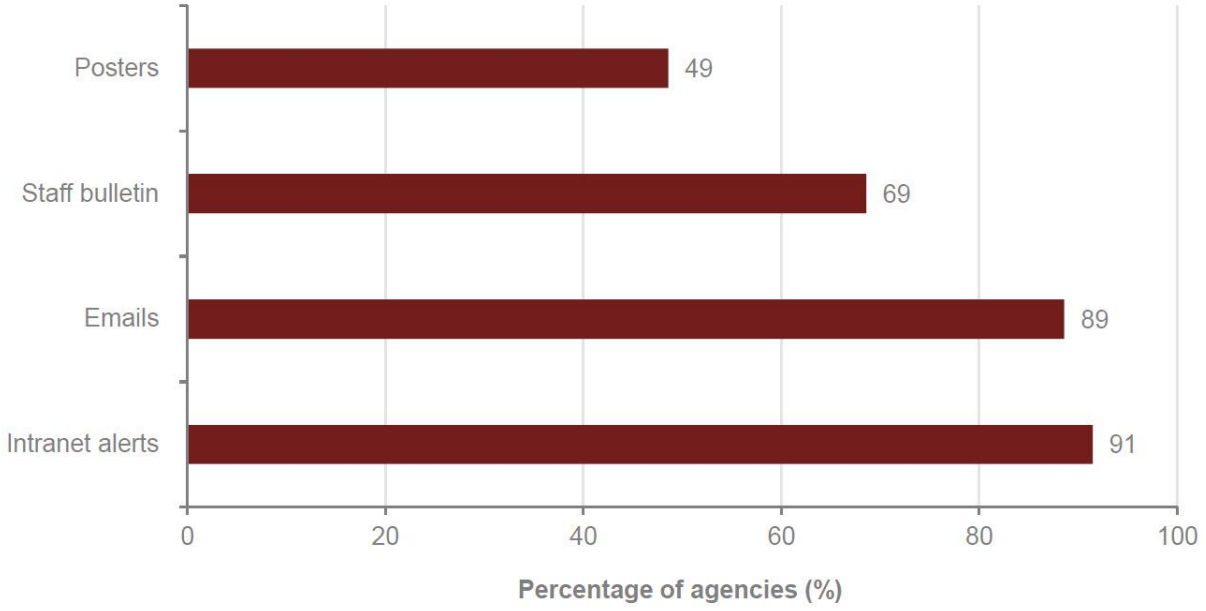
Agencies should continue to provide training and awareness to help manage data breaches

Seventy per cent of agencies have provided training to employees in relation to data protection and breach management, with a specific focus on new starters. Eighty-one per cent of these agencies continue to provide on-going training to staff.

Data breach management awareness training helps agencies reduce the risk of data breaches occurring due to human error, and increase the detection of data breaches. Training ensures employees:

- understand the risks to the agency (both financial and reputational)
- are aware of policies and procedures for data breach management
- have the ability to identify potential breaches when they occur
- understand the importance of de-identifying sensitive data where release of certain information is required or appropriate
- consider contextual information, which may still allow individuals to be identified, even after the data is de-identified
- report potential breaches in a timely manner.

The graph below details the different methods agencies use to create awareness of data breaches.



Awareness activities (of the 90% of agencies with other awareness activities)

Detecting and responding to cyber security incidents performance audit[7] – published 2 March 2018

The NSW Government relies on digital technology to deliver services, organise and store information, manage business processes, and control critical infrastructure. The increasing global interconnectivity between computer networks has dramatically increased the risk of cyber security incidents. Such incidents can harm government service delivery and may include the theft of information, denial of access to critical technology, or even the hijacking of systems for profit or malicious intent.

This audit examined cyber security incident detection and response in the NSW public sector. It focused on the role of the Department of Finance, Services and Innovation (DFSI), which oversees the Information Security Community of Practice, the Information Security Event Reporting Protocol, and the Digital Information Security Policy (the Policy).

The audit also examined ten case study agencies to develop a perspective on how they detect and respond to incidents. We chose agencies that are collectively responsible for personal data, critical infrastructure, financial information and intellectual property.

Conclusion

There is no whole-of-government capability to detect and respond effectively to cyber security incidents. There is limited sharing of information on incidents amongst agencies, and some of the agencies we reviewed have poor detection and response practices and procedures. There is a risk that incidents will go undetected longer than they should, and opportunities to contain and restrict the damage may be lost.

Given current weaknesses, the NSW public sector's ability to detect and respond to incidents needs to improve significantly and quickly. DFSI has started to address this by appointing a Government Chief Information Security Officer (GCISO) to improve cyber security capability across the public sector. Her role includes coordinating efforts to increase the NSW Government's ability to respond to and recover from whole-of-government threats and attacks.

Key findings

Agency incident detection and response approaches range from good to poor

Two case study agencies have good detection and response processes and four have a low capability to detect and respond to incidents in a timely manner. The remaining four have a medium capability.

Most use an automated tool for detecting and alerting IT administrators when there is a suspected incident. The tool's coverage ranged from all IT systems in some agencies to just a few in others. Some agencies do not use such a tool and only monitor logs periodically or on an ad hoc basis.

Most case study agencies have incident response procedures, although some lack guidance on who to notify and when, such as when an incident would need to be reported to the chief executive. Some agencies do not have response procedures at all. This would limit their ability to minimise business damage caused by a cyber security incident. Eight agencies had not tested their procedures, presenting a risk they may not work well during a real cyber incident.

Some case study agencies advised they review the effectiveness of their response to cyber security incidents, but could only provide limited evidence to support this. Post-incident reviews of incident response help identify and resolve any deficiencies in procedures and practice.

Most IT service providers are not contractually obliged to report incidents to agencies

Agencies advise that IT service providers report cyber security incidents to them, but only two of ten had contractual arrangements which obliged providers to report incidents in a timely manner. Agencies without such arrangements have little assurance that they are advised of all significant

[7] https://www.audit.nsw.gov.au/our-work/reports/detecting-and-responding-to-cyber-security-incidents-

incidents in a timely way. Where agencies are not informed of an incident, they cannot act to contain the incident and limit damage to themselves and their stakeholders.

Training is limited and role requirements and responsibilities in agencies are unclear

Case study agencies could provide limited evidence of what cyber security training had been provided to their staff. Most agencies indicated that key staff had been trained in incident procedures, but only one agency was able to provide any training records to support these claims.

Cyber security incidents can start as simply as an individual opening a fraudulent website or email and unwittingly allowing unauthorised access to IT systems. Awareness training can reduce this risk, but few agencies undertake regular training or keep their staff up-to-date on these and other types of cyber security attack.

Case study agencies could provide little documentation on the role requirements and responsibilities of their staff to support an effective detection and response capability. Incident detection and response are likely to be less effective if roles and responsibilities are not clear.

Sharing of cyber security intelligence is limited

Two case study agencies did not report incidents to DFSI even though it is mandatory for them to do so. Three other agencies that are required to report advised they had no incidents but would not report even if they did. None of the agencies' procedures included a requirement to report incidents to DFSI.

Most of the case study agencies saw little benefit in reporting incidents to DFSI. This limits DFSI's ability to coordinate a whole-of-government response and support agencies to properly manage cyber security incidents. DFSI guidelines are weak on which incidents should be reported and when. There is also no reporting template to assist agencies to report incidents in a consistent and timely way. There are limited avenues for sharing information amongst agencies after incidents have been resolved, meaning the public sector may be losing valuable opportunities to improve its protection and response.

DFSI does not have a clear mandate or capability to ensure effective detection and response across the NSW public sector

The Policy sets out a range of requirements for public service agencies regarding detection and response. There is a lack of adherence by agencies to the policy, and it should be enforced. DFSI does not have a clear mandate to enforce it.

It does not have a clear mandate to assess whether agencies have an acceptable detection and response capability. It is also not able to ensure agencies report incidents to it to enable effective sharing of information across the public sector and inform whole-of-government responses.

DFSI has not allocated resources to gather or process incoming threat intelligence and communicate it across government. During an incident impacting multiple agencies this could reduce the NSW public sector's ability to respond quickly and appropriately. However, it has begun to build such a capacity through the appointment of the GCISO.

When incidents have been reported to DFSI, it has not provided dedicated resources to assess them and coordinate the public sector’s response. There are currently no requirements for DFSI to respond to incidents impacting multiple agencies and no guidance on what it is meant to do if such an incident is reported. The lack of central response coordination risks delays and damage spreading further. There is also little or no post-incident review, including lessons learnt.

Recommendations

As a matter of priority, the Department of Finance, Services and Innovation should:

1. develop whole-of-government procedures, protocol and supporting systems to effectively share reported threats and respond to cyber security incidents impacting multiple agencies, including post-incident reviews and communicating lessons learnt
2. assist agencies to improve their detection and response by providing:
    - better practice guidelines for incident detection, response and reporting to help agencies develop their own practices and procedures

- training and awareness programs, including tailored programs for a range of audiences such as cyber professionals, finance staff, and audit and risk committees
- role requirements and responsibilities for cyber security across government, relevant to the size and complexity of each agency
- a support model for agencies that have limited detection and response capabilities

3. revise the Digital Information Security Policy and Event Reporting Protocol by:
   - clarifying what security incidents must be reported to DFSI and when
   - extending mandatory reporting requirements to those NSW Government agencies not currently covered by the policy and protocol, including State owned corporations
4. develop a means for agencies to report incidents in a more effective manner, such as a secure online template, that allows for early warnings and standardised details of incidents and remedial advice
5. enhance NSW public sector threat intelligence gathering and sharing including formal links with Australian Government security agencies, other states and the private sector
6. direct agencies to include standard clauses in contracts requiring IT service providers to report all cyber security incidents within a reasonable timeframe
7. provide assurance that agencies have appropriate incident reporting procedures by:
   - extending the attestation requirement within the Digital Information Security Policy to cover procedures and reporting
   - reviewing a sample of agencies' incident reporting procedures each year.