auditoffice
OF NEW SOUTH WALES

Detecting and responding to cyber security incidents

2 MARCH 2018

NEW SOUTH WALES AUDITOR-GENERAL'S REPORT

PERFORMANCE AUDIT

THE ROLE OF THE AUDITOR-GENERAL

The roles and responsibilities of the Auditor-General, and hence the Audit Office, are set out in the *Public Finance and Audit Act 1983* and the *Local Government Act 1993*.

We conduct financial or 'attest' audits of State public sector and local government entities' financial statements. We also audit the Total State Sector Accounts, a consolidation of all agencies' accounts.

Financial audits are designed to add credibility to financial statements, enhancing their value to end-users. Also, the existence of such audits provides a constant stimulus to entities to ensure sound financial management.

Following a financial audit the Audit Office issues a variety of reports to entities and reports periodically to parliament. In combination these reports give opinions on the truth and fairness of financial statements, and comment on entity compliance with certain laws, regulations and government directives. They may comment on financial prudence, probity and waste, and recommend operational improvements.

We also conduct performance audits. These examine whether an entity is carrying out its activities effectively and doing so economically and efficiently and in compliance with relevant laws. Audits may cover all or parts of an entity's operations, or consider particular issues across a number of entities.

As well as financial and performance audits, the Auditor-General carries out special reviews and compliance engagements.

Performance audits are reported separately, with all other audits included in one of the regular volumes of the Auditor-General's Reports to Parliament – Financial Audits.

GPO Box 12
Sydney NSW 2001

The Legislative Assembly
Parliament House
Sydney NSW 2000

The Legislative Council
Parliament House
Sydney NSW 2000

In accordance with section 38E of the *Public Finance and Audit Act 1983*, I present a report titled '**Detecting and responding to cyber security incidents'.**

Margaret Crawford
Auditor-General
2 March 2018

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au

contents

Detecting and responding to cyber security incidents

Section one

Detecting and responding to cyber security incidents

Executive summary

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.

1. 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 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.

2. 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.

1. Introduction

1.1 Background

Recent global security incidents and the attack on the Australian Census highlight the importance of systems and processes for detecting and responding effectively to security incidents for NSW Government agencies.

A cyber security incident, for the purposes of this audit, is a past or ongoing intrusion, disruption, or other event that impairs the confidentiality, integrity, or availability of electronic information, information systems, services, or networks. Cyber incidents include major events impacting other jurisdictions, even if they do not directly impact NSW public sector agencies or universities.

Incident detection can be difficult. The Verizon 2017 Data Breach investigations report, with input from 65 organisations including the US Federal Bureau of Investigation and Australian Federal Police, found that the timeline from breach to discovery is over 12 months for 60 per cent of incidents reported in public sector organisations.

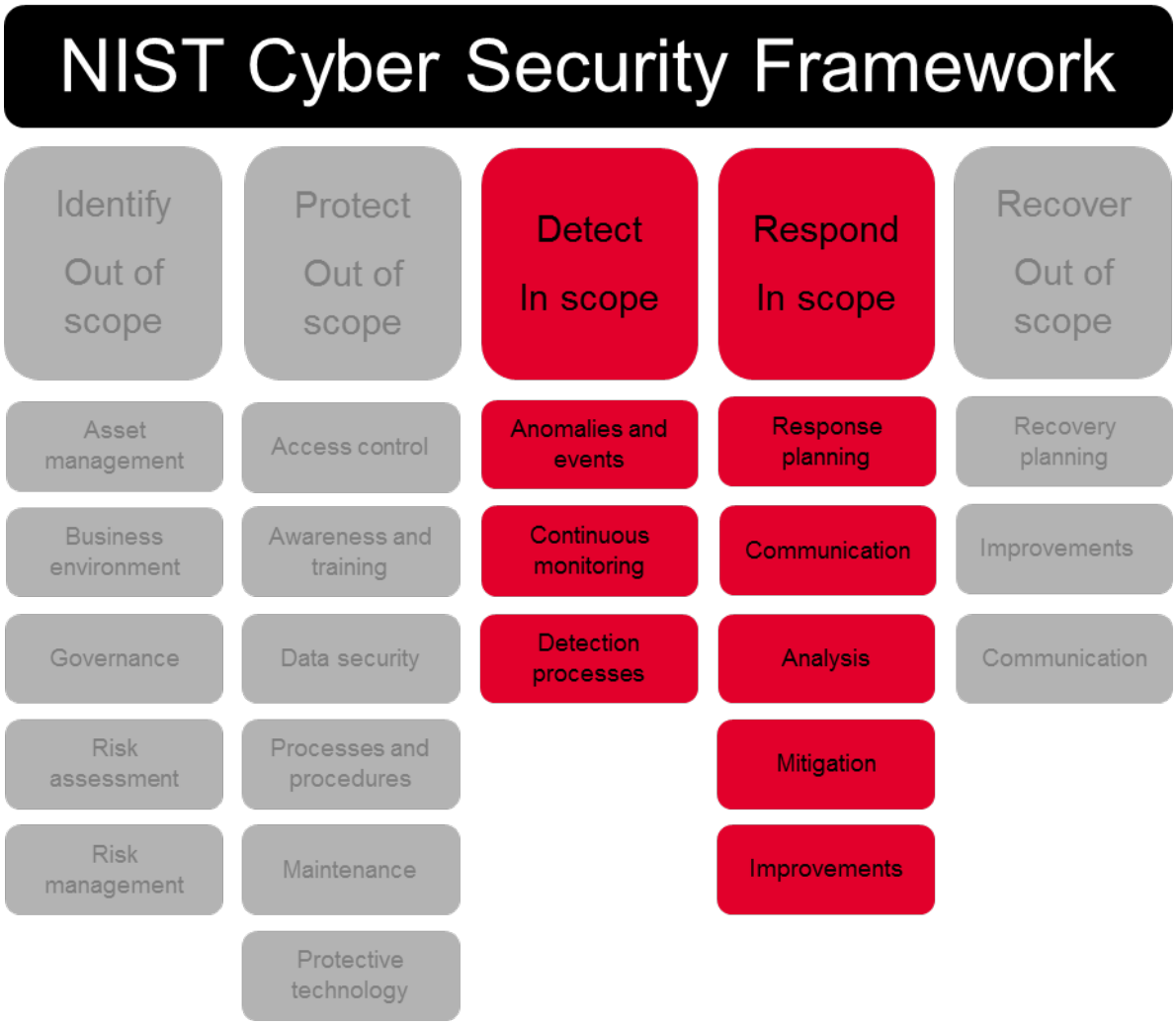
This audit assessed cyber security incident detection and response in the NSW public sector. It focused on the role of the Department of Finance, Services and Innovation (DFSI) which oversees the NSW Information Security Community of Practice, the Information Security Event Reporting Protocol and the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

It examined ten case study agencies to develop a whole-of-government perspective on how well agencies detect and respond to incidents. We chose agencies that should have a strong detection and response capability as they are collectively responsible for personal data, critical infrastructure, financial information and intellectual property.

Aspects of cyber security addressed in this report

In 2013, the US National Institute of Standards and Technology (NIST) developed a cyber security framework to provide an effective approach to managing cyber security risk for critical infrastructure services. The framework consists of five functions - Identify, Protect, Detect, Respond, Recover - that provide a high-level, strategic view of an organisation's management of cyber security risk. There is a range of frameworks available for managing cyber security. The NIST framework provides a convenient overview of cyber security functions. The following diagram indicates which two of these functions are within the scope of this audit and the three functions which are out of scope.

Exhibit 1 – NIST Cyber Security Framework Core and Implementation Tiers



Source: NIST / Audit Office 2017.

The Digital Information Security Policy and ISO 27001

The NSW Government has established its ICT Strategy to improve service delivery and derive better value from its investments. As part of the ICT Strategy, the Policy sets out the security requirements for digital information in NSW public service agencies. The Policy does not apply to State owned corporations, local councils and universities, although it is recommended for adoption.

A key objective of the Policy is to 'provide assurance to NSW Parliament and the people of New South Wales that information held by the government is appropriately protected and handled'. The Policy has a broad range of requirements for agencies that includes:

- reporting on information security events, incidents, near misses and weaknesses
- establishing a collaborative approach to information security by sharing information security experience and knowledge.

The Policy requires agencies to manage information security according to the International Standard – ISO 27001 'Information technology – Security techniques – Information security management systems – Requirements'. ISO 27001 contains a range of requirements including the need to ensure that detection, prevention and recovery controls be implemented to contain a security incident.

Information Security Community of Practice and Event Reporting Protocol

The Community of Practice is intended to provide an opportunity for information security managers to exchange ideas and experiences. The community is made up of senior responsible officers for IT security and operational level IT staff from across NSW Government and meets on a regular basis.

The Information Security Event Reporting Protocol outlines the process for sharing information on cyber security events and incidents. The key steps outlined in the protocol are:

- **Identify**: Senior Responsible Officers (SROs) identify or are informed of the information security event or incident
- **Act**: SROs take action to address the information security event or incident, including assessing severity and impact, notifying the relevant agency authority, and taking remedial action
- **Communicate**: SROs alert the Information Security Community of Practice immediately on govdex and by email (govdex is a secure cross agency online portal for document and information sharing. Shared information includes security alerts, upcoming IT security industry events and industry reports).

Whole-of-government reporting on cyber security maturity

The Policy requires NSW public service agencies to provide DFSI with an annual progress report on their maturity and the effectiveness of their information security management system. Agencies are required to rate themselves from one to five against 12 'actions'. Appendix 2 provides the list of actions and a model for how agencies are required to rate themselves.

The key actions most relevant to incident detection and response are:

- Action 4 - Access to digital information and digital information systems is monitored and controlled
- Action 11 - Processes are in place for the communication of digital information security events and weaknesses associated with digital information systems within the agency and across the sector as appropriate
- Action 12 - Awareness training program is implemented and maintained.

In 2016, DFSI commissioned a survey of cyber security maturity (the 2016 survey) across all ten primary cluster departments and a selection of 21 additional agencies to provide a representative sample that included large, medium and small agencies. The survey was designed to deliver a high-level overview of cyber security capability for threat prevention, detection and response across the NSW public sector. It was supplemented with interviews of key agency staff to further improve understanding. Some of the survey results are discussed in this report.

Appointment of GCISO

In March 2017, the NSW Government announced the appointment of its first Government Chief Information Security Officer (GCISO). The GCISO's role is to ensure a collaborative approach to cyber security by working with NSW Government agencies, Australian, State and international governments, industry and research groups, and to develop a set of standards for the NSW public sector.

At the NSW Government level, the GCISO's role is to coordinate information security and cyber practices across agencies including creating better governance and accountability, sharing of threat intelligence and working to reach agreement on minimum standards.

2. Agency detection and response

Some of our case study agencies had strong processes for detection and response to cyber security incidents but others had a low capability to detect and respond in a timely way.

Most agencies have access to an automated tool for analysing logs generated by their IT systems. However, coverage of these tools varies. Some agencies do not have an automated tool and only review logs periodically or on an ad hoc basis, meaning they are less likely to detect incidents.

Few agencies have contractual arrangements in place for IT service providers to report incidents to them. If a service provider elects to not report an incident, it will delay the agency's response and may result in increased damage.

Most case study agencies had procedures for responding to incidents, although some lack guidance on who to notify and when. Some agencies do not have response procedures, limiting their ability to minimise the business damage that may flow from a cyber security incident. Few agencies could demonstrate that they have trained their staff on either incident detection or response procedures and could provide little information on the role requirements and responsibilities of their staff in doing so.

Most agencies' incident procedures contain limited information on how to report an incident, who to report it to, when this should occur and what information should be provided. None of our case study agencies' procedures mentioned reporting to DFSI, highlighting that even though reporting is mandatory for most agencies their procedures do not require it.

Case study agencies provided little evidence to indicate they are learning from incidents, meaning that opportunities to better manage future incidents may be lost.

Recommendations

The Department of Finance, Services and Innovation should:

- assist agencies 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 size and complexity of each agency
  - a support model for agencies that have limited detection and response capabilities
- revise the Digital Information Security Policy and Information Security 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.

2.1 Agency incident detection

Only two case study agencies have a high detection capability

Most case study agencies had processes in place for scanning for cyber security events and incidents. These included monitoring firewall logs, server logs, web filtering and antivirus software, and alerts and reports from IT service providers. Most also use a Security Information and Event Management (SIEM) tool which analyses security logs produced by network hardware and applications, and generates alerts on possible cyber security events and incidents. Automated tools are necessary as it is not feasible for IT administrators to manually review the large numbers of computer logs being generated. These tools alert IT administrators when there is a suspected incident to investigate.

The range of coverage for the SIEM tools varies from 100 per cent of IT systems in some agencies we reviewed to just a few key systems in others. Two of the case study agencies do not have access to a SIEM tool and only review their logs and alerts periodically or on an ad hoc basis. Overall, this means that some case study agencies only have partial coverage of IT systems, limiting their ability to detect incidents across the full range of their information systems.

Requirement	The Policy requires that access to digital information and digital information systems be monitored and controlled.
Standard	ISO 27001 requires that detection, prevention and recovery controls be implemented to contain a security incident.

The following table indicates the range of detection capability for the ten case study agencies.

Exhibit 2 – Intrusion detect capability across ten case study agencies

Agency	Intrusion detection - as reported by agencies	Audit Office assessment
Agency A	Security Incident and Event Management (SIEM) tool with 100 per cent of IT systems monitored.	High capability of detecting incidents
Agency B	SIEM tool with 100 per cent of (locally hosted) IT systems monitored.	High capability of detecting incidents
Agency C	SIEM tool with monitoring of key systems only.	Medium capability of detecting incidents
Agency D	SIEM tool with 80 per cent of IT systems monitored.	Medium capability of detecting incidents
Agency E	SIEM tool with 68 per cent of IT systems monitored.	Medium capability of detecting incidents
Agency F	SIEM as part of Security Operations Centre (SOC) provided by a service provider for another agency with 100 per cent of key systems monitored. Some local systems are not covered by the SIEM.	Medium capability of detecting incidents
Agency G	SIEM tool as part of a SOC, provided by a vendor, monitoring IT infrastructure but not applications.	Low/medium capability of detecting incidents
Agency H	Network Operation Centre (24/7) from the vendor for the core of this agency's infrastructure with a SIEM planned for 2019. Corporate systems (and SIEM) are provided by another agency with the SIEM covering around a third of IT systems.	Low capability of detecting incidents
Agency J	SIEM tool provided by another agency, monitoring a portion of key IT systems. Some local systems are not covered by the SIEM tool.	Low capability of detecting incidents
Agency K	Alerts generated by IT systems are reviewed on an ad hoc basis. Additional monitoring is provided by vendors during important business periods.	Very low detection capability

Source: Audit Office 2017.

The above data on intrusion detection coverage was self-reported by each agency. Eight agencies provided evidence that they had a SIEM tool, five agencies provided a list of systems they claim are monitored by their tool, but only one could provide clear evidence of the number of IT systems monitored by their tool. This indicates agencies may have limited ability to check the actual levels of coverage being provided by their SIEM tool, relying instead on contractual arrangements and advice from IT service providers.

Only one case study agency had procedures identifying responsibilities for detecting cyber incidents. This could mean that staff do not know who is responsible or that incidents could easily be missed due to some areas or systems not being covered.

Six of the ten case study agencies' procedures include guidelines on what constitutes a cyber security incident but only one agency's procedures discussed the methods it uses to detect incidents. Four agencies have procedures that require event logs and real-time alerts to be reviewed. Nine of the ten agencies could not provide documents or plans on how they detect security incidents.

As all case study agencies are responsible for important data or infrastructure, a medium or low detection capability is a concern as undetected incidents have the potential to not only damage that agency but to spread and impact other agencies.

Issues identified with detection capability in case studies are likely to be more widespread

The 2016 survey conducted for DFSI revealed that many public sector agencies are only partially effective at detecting cyber security incidents. For example:

- around half the responding agencies did not have a SIEM tool, whereas only two of the ten case study agencies did not have access to a SIEM tool
- a significant number of agencies (particularly smaller agencies) did not have a dedicated security monitoring capability, presenting a risk that certain types of attack remain undetected for a prolonged period
- a small number of agencies have no intrusion detection capability.

Of the agencies that self-reported to DFSI in 2017, over two-thirds indicated they had a medium to low maturity in relation to whether 'access to digital information and digital information systems is monitored and controlled.' This means that these agencies are only partially effective at detecting security incidents.

Most contractual arrangements do not require IT service providers to report incidents

Where IT services are delivered by an external provider, cyber security incidents may be solely managed by the service provider without the agency's knowledge. This is largely because most contractual agreements do not specify that incidents are to be reported to the agency, nor when this should occur.

IT service providers to only two agencies were contractually obligated to report significant incidents as soon as possible after detection. One agency did have a service level agreement with a security provider requiring reporting of significant incidents within two days of resolution. Another agency had access to a web portal with information on security incidents detected, and real-time access to situation briefings during critical incidents.

Without a contractual arrangement which requires prompt reporting, an agency may not be notified in time to contain damage to business processes and reputation, and harm to the public such as the loss of personal information.

Requirements

- The Policy requires that shared ownership and responsibility for managing the digital information and digital information systems should be clearly outlined in any contractual or service level agreements with IT service providers.
- It also states that agencies that manage risk with outsourced service providers must be satisfied that providers have sufficient controls in place to adequately ensure the security of digital information and information systems.

Even though all ten case study agencies indicated they are being notified of events, incidents and imminent threats, they cannot be certain of being notified of all incidents. The likelihood of not being notified is greater without contractual obligations in place.

DFSI has recently implemented a revised contract template, for agencies engaging in IT contracts over $150,000, that includes the need for IT service providers to report security issues to agencies immediately and conduct an investigation. It has taken steps to communicate the new requirements across the public sector, although it does not follow-up with agencies to ensure agencies are using the templates.

IT service provider communication is generally poor

Only a few case study agencies have regular meetings with service providers and receive reports on security events, incidents detected, and response to events. Seven agencies advised they routinely receive security performance reports from their IT service provider, however only five were able to provide any evidence to support this.

The most effective security reports we reviewed contain information on security events and incidents from multiple detection sources such as email filtering, antivirus software and vulnerability scanning of servers. One agency report also included information on progress with its IT systems patching program, including work that was still unresolved. The weakest reports only provided a list of events with no analysis or detail about remedial action.

Agencies could have greater confidence that service providers are delivering an effective detection service if they held regular meetings with and obtained regular reports from their IT security service providers.

Some agencies rely on other agencies to detect incidents but without formal agreements

Three case study agencies rely almost entirely on other larger agencies for incident detection, but have no formal agreements in place to support these arrangements. The lack of formal agreements increases the risk that agencies will not be notified in the event of an incident, even though they continue to retain responsibility for business processes and the liability for any security breach.

The response from the other agency providing the security services may not be as comprehensive and effective without a memorandum of understanding, or other form of agreement, which clarifies the responsibilities of each party.

2.2 Agency incident response

Some response procedures are incomplete and most have never been tested

The ability of some case study agencies to minimise damage during a cyber security incident is compromised because they do not have comprehensive incident response procedures.

Five of the ten case study agencies have detailed response procedures, although only two have tested their procedures. Untested procedures and untrained staff increase the risk that an inadequate or incorrect response is put in place during a cybersecurity incident.

Five case study agencies have no detailed response procedures. Three agencies referred us to other agencies providing incident response capabilities on their behalf, although without formal agreements in place to support this function. Two other agencies referred us to documentation provided by IT service providers.

Only one agency maintains its own 24/7 incident response capability. Most agencies engage third-party providers who provide a response capability for major incidents, and not all are 24/7.

Requirement	The Policy requires that internal processes must be in place for the communication of digital information security events, incidents, near misses and weaknesses associated with digital information systems, and timely corrective action must be taken.
Standard	ISO 27001 requires the establishment of management responsibilities and procedures to ensure a quick, effective and orderly response to information security incidents. It also requires documented procedures for responding to information security breaches.

The Australian Government's Information Security Manual (ISM) describes controls that Australian Government agencies are required to include in incident response documentation. NSW agencies would also benefit from the inclusion of controls, listed in the following table, in their procedures. These results indicate there is significant scope for improvement in agencies' incident response procedures.

Exhibit 3 – Agency response procedures

Procedures and policies include:	Number of case study agencies demonstrating the ISM control
Broad guidance on what constitutes a cyber security incident	6/10
Clear definitions of the types of cyber security incidents that are likely to be encountered	3/10
The expected response to each cyber security incident type	1/10
Steps necessary to ensure that critical systems remain operational	2/10
Steps necessary to ensure the integrity of evidence supporting the response to a cyber security incident	4/10
The minimum level of cyber security incident response and investigation training for users and system administrators	1/10

Source: Audit Office 2017.

All agencies should be ensuring that they have comprehensive procedures in place for responding to cyber security incidents. These procedures should address the containment of both IT and business risk, recognising that IT service providers may play a key role in responding to a cyber security incident, but do not bear ultimate responsibility.

Limited training and awareness may hamper incident response

The case study agencies could only provide limited information on the training and awareness of their staff to support an effective detection and response capability. 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.

Requirement	The Policy requires that employees doing work that affects information security performance must take the initiative to remain aware of changes and maintain their skills through training and education, where necessary.
Standard	ISO 27001 requires that all employees of an organisation shall receive appropriate awareness education and training, and regular updates on organisational policies and procedures, as relevant for their job function. It also requires that detection, prevention and recovery controls to protect against malware (i.e. malicious software) be implemented, combined with appropriate user awareness.

One agency indicated that none of its staff had received training in incident detection and response, instead referring to another agency providing them with an incident detection and response capability. Only one of the case study agencies provided documentation on the minimum level of cyber security incident response and investigation training for users and system administrators.

Cyber security incidents can start with an individual unwittingly opening a fraudulent website or email and allowing unauthorised access to IT systems. Awareness training could reduce the number of cases of human error, but few of the case study agencies undertake regular training and do not keep their staff up-to-date on these and other types of cyber security attack.

These findings are consistent with the Audit Office of New South Wales' 2017 Internal Controls and Governance audit of 39 large agencies tabled in the NSW Parliament on 20 December 2017. The audit found that around a quarter of agencies provide no training in cyber security awareness and had not identified staff most at risk of cyber-attack.

The need for training and cyber security awareness is well recognised and should be taken seriously by all agencies. The Australian Government's ISM states that many potential cyber security incidents are noticed by personnel rather than software tools. However, this can only occur effectively if personnel are well trained, aware of information security issues and know how to recognise potential incidents.

Of the agencies that self-reported to DFSI in 2017, over two-thirds indicated they had a medium to low maturity in relation to whether an awareness training program is implemented and maintained. This means they do not have an effective awareness program and the NSW public sector is carrying unnecessarily high risk of staff unwittingly contributing to a security incident.

Service providers assist agencies to respond but do not carry ultimate responsibility

IT service providers play an important role in assisting agencies to respond to cyber security incidents, including providing technical advice. However, case study agencies' response procedures do not specifically recognise the role of IT service providers, meaning it is unclear who is accountable for each aspect of a response. Three agencies do not have their own response procedures, relying instead on procedures provided by service providers.

Cyber risk is a business risk, not just a technical risk, hence it is poor practice for even a small agency to claim that management of cyber risk and response to incidents is entirely the IT service provider's problem. Every agency needs to develop its own procedures for responding to an incident related to its core business. An IT service provider can respond to a technical issue, but managing the impact on the business is the agency's responsibility.

In addition, contracts with IT service providers do not contain minimum requirements for providing advice. The contracts also do not include a right to audit or the provision of independent assurance to allow agencies to investigate whether they are getting the levels of service specified in the contract.

Agency staff have limited guidance on reporting cyber incidents

Knowing who to notify about a cyber security incident is important so the right people can be involved at the right time to mitigate damage. Of the procedures provided by the ten case study agencies:

- only two detailed what information should be provided at each point in an incident, and when communication should take place. Only one provided details of the communication required for each type of incident
- six included information on reporting within the agency but did not include reporting to any external bodies. None included a requirement to report incidents to DFSI
- four clearly identified when incidents are to be elevated to senior management, although none explained the level of detail on each incident that should be reported to the chief executive, the board or the audit and risk committee
- only two considered public relations and media engagement, which means agencies may struggle to manage community expectations and reputational damage in the event of a major incident.

Requirement	The Policy requires that agencies maintain appropriate contacts with relevant authorities during security incidents. Internal processes must be in place for communicating digital information security events, incidents, near misses and weaknesses associated with digital information systems.
Standard	ISO 27001 requires information security events be reported through appropriate management channels as quickly as possible. It also states that information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

Role requirements and responsibilities are unclear

Case study agencies could only provide limited information to show the role requirements and responsibilities of their staff are clear and well communicated to support an effective detection and response capability.

Requirement

The Policy requires that employees doing work that affects information security performance understand the responsibilities of their role. It also states that governance arrangements must include a designated individual responsible for digital security who has relevant information security expertise.

Incident response is likely to be less effective where role requirements and responsibilities are unclear. Four of our case study agencies were unable to provide information on the names and responsibilities of key staff involved in responding to incidents. The other six agencies could only provide partial information on names and responsibilities of staff involved in IT security. Role requirements and responsibilities were also vague in incident response procedures.

There are currently few standard role descriptions for cyber/information security positions across government agencies, although the Public Service Commission has done some work on this. For example, the Chief Information Security Officer role has not been standardised across government departments, with some only advising on policy rather than being responsible for implementing policy.

Case study incident highlighting poor communication

The following is a timeline for a 2017 attempted financial fraud that impacted a case study agency (Agency Y) and another agency (Agency X), which provides IT systems for Agency Y. The intent of the cyber criminals was to gather financial staff credentials to create fraudulent payments. The incident initially impacted only Agency Y and Agency X, but spread to other agencies, at which point it was reported to DFSI.

Exhibit 4 – Timeline for an attempted financial payment fraud incident using email phishing

Day	Activity
Day 0	First email account in Agency Y is compromised
Day 6	The compromised account in Agency Y sends phishing emails (i.e. deceptive emails) attempting to gain the credentials of finance staff
Day 14	Agency X detects a fraudulent invoice and informs Agency Y
Day 15	Agency X raises the phishing incident to major status and contacts a security vendor for assistance
Day 17	Agency X asks Agency Y to tell its compromised email account users to change their passwords
Day 20	A compromised email account in Agency Y sends out 450 phishing emails, some of which are directed to other NSW public sector agencies
Day 28	Agency X informs Agency Y that 300 email users have clicked on the link in the phishing email
Day 30	Agency Y's payments gateway is closed to prevent fraudulent payments
Day 31	Agency Y identifies around 200 email accounts that are now under the control of financial criminals
Day 31	Agency Y tells impacted email account users to change their passwords, but does not secure (temporarily lock) the email accounts
Day 35	Agency Y's financial staff realise they cannot make payments, including business invoices, staff salaries and superannuation because the gateway had been shut
Day 36	Another agency advises Agency X that it cannot access X's systems. Agency X reports the incident to GCISO
Day 42	Agency X asks Agency Y to check on the password of the first compromised account. Agency Y finds that the account is still compromised
Day 49	Agency Y's payments gateway is re-opened.

Source: Audit Office 2017.

The incident was resolved by closing the payments gateway, blocking access from suspicious overseas IP addresses and resetting passwords to prevent the hackers from continuing to access accounts. An investigation is currently ongoing.

The delays in controlling the incident highlight a lack of communication within the organisation and a lack of communication between the agencies involved. Reporting to DFSI eventually took place, but only after the Agency X realised the incident had potentially spread to other agencies. During this 36-day delay, the GCISO was not able to forewarn other public sector agencies. Very little information was provided to the chief executives or the audit and risk committees in either Agency Y or Agency X.

This incident could have been resolved much sooner if agency Y had implemented comprehensive incident response procedures. Such procedures would have included business processes to contain the impact, such as shutting down compromised email accounts, and implementing more rigorous forms of authentication to prevent the criminals from continuing to hack the email accounts and distribute fraudulent emails.

This incident demonstrates a lack of training and awareness, deficiencies in preventative controls and a lack of clear response procedures. It is also an example of insufficient information being provided to executives to enable them to adequately consider the allocation of resources to mitigate risk. The incident highlights the importance of reporting to DFSI so other agencies can be aware of the incident and can protect their part of the public service network.

Of the agencies that self-reported to DFSI in 2017, over two-thirds indicated they had a medium to low maturity in relation to whether: ‘processes are in place for the communication of digital information security events and weaknesses associated with digital information systems within the agency and across the sector as appropriate.’ This indicates they are only partially effective at communicating events and incidents. A lack of communication will limit their ability to ensure security levels meet government and public expectations.

Limited effort to learn from incidents means future incidents may not be managed better

Case study agencies could provide limited evidence that they review the effectiveness of their response to incidents to identify improvements in practice that will help avoid future harm and improve their response to cyber incidents.

Standard

ISO 27001 requires that knowledge gained from analysing and resolving information security incidents be used to reduce the likelihood or impact of future incidents.

The purpose of recording cyber security incidents in a register is to highlight their nature and frequency so that corrective action can be taken. This information can subsequently be used as an input into future security risk assessments of systems. For example, the Australian Government uses cyber security incident reports as the basis for identifying and responding to cyber security events, and for developing new policies, procedures, techniques and training measures to prevent the recurrence of similar incidents across government.

All of the case study agencies have documentation that includes a requirement to conduct post-incident analysis, although only one agency could provide an example of a detailed incident review. Only one agency had plans that discuss incidents and lessons learned.

If agencies do not follow-up incidents they may not be able to identify deficiencies in their controls and act to limit or avoid the harm from future incidents.

3. Whole-of-government response

DFSI lacks a clear mandate or capability to provide effective detection and response support to agencies, and there is limited sharing of information on cyber security incidents.

DFSI does not currently have a clear mandate and the necessary resources and systems to detect, receive, share and respond to cyber security incidents across the NSW public sector. It does not have a clear mandate to assess whether agencies have an acceptable detection and response capability. It is aware of deficiencies in agencies and across whole-of-government, and has begun to conduct research into this capability.

Intelligence gathering across the public sector is also limited, meaning agencies may not respond to threats in a timely manner. DFSI has not allocated resources for gathering of threat intelligence and communicating it across government, although it has begun to build this capacity.

Incident reporting to DFSI is mandatory for most agencies, however, most of our case study agencies do not report incidents to DFSI, reducing the likelihood of containing an incident if it spreads to other agencies. When incidents have been reported, DFSI has not provided dedicated resources to assess them and coordinate the public sector's response. There are currently no formal requirements for DFSI to respond to incidents and no guidance on what it is meant to do if an incident is reported. The lack of central coordination in incident response risks delays and increased damage to multiple agencies.

DFSI's reporting protocol is weak and does not clearly specify what agencies should report and when. This makes agencies less likely to report incidents. The lack of a standard format for incident reporting and a consistent method for assessing an incident, including the level of risk associated with it, also make it difficult for DFSI to determine an appropriate response.

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.

Recommendations

The Department of Finance, Services and Innovation should:

- develop whole-of-government procedure, protocol and supporting systems to effectively share reported threats and respond to cyber security incidents impacting multiple agencies, including follow-up and communicating lessons learnt
- develop a means by which agencies can 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
- enhance NSW public sector threat intelligence gathering and sharing including formal links with Australian Government security agencies, other states and the private sector
- direct agencies to include standard clauses in contracts requiring IT service providers report all cyber security incidents within a reasonable timeframe
- provide assurance that agencies have appropriate reporting procedures and report to DFSI as required by the policy and protocol by:
  - extending the attestation requirement within the DISP to cover procedures and reporting
  - reviewing a sample of agencies' incident reporting procedures each year.

3.1 Incident detection and reporting across the NSW public sector

There is no whole-of-government detection capability, limiting DFSI's ability to support agencies

DFSI does not currently have the capability and capacity to detect cyber security events and incidents across the NSW public sector, limiting its ability to support agencies. It has not yet developed this capability because it does not have a clear mandate for detecting cyber incidents across the NSW public sector. Although the Digital Government Strategy pledges to strengthen risk management and response by building a whole-of-government cyber security capability, in practice agencies have not interpreted this to mean DFSI has a mandate for detection. Currently, responsibility for detecting and reporting on cyber security incidents sits with individual agencies. However, the previous chapter indicated that not all agencies have a strong detection capability.

This contrasts with the Australian, Queensland and South Australian Governments which provide some form of whole-of-government detection capability, such as monitoring internet gateways. Of all incidents reported to DFSI in the past two years, 25 per cent were not reported by the affected agency, but instead by the Australian Cyber Security Centre (ACSC) through its monitoring of traffic to and from Australian Government websites. The ACSC advised that it has access to a range of information and partnerships to assist in identifying incidents. However, it does not routinely pick up events that do not involve an Australian Government agency.

Either NSW agencies did not detect these incidents or, if they did detect them, they did not resolve them prior to ACSC detecting them. This unintended reliance on external parties to detect some incidents in an ad hoc manner, rather than detection by the NSW public sector and its IT service providers, increases the time between incident initiation and response by the impacted agency.

DFSI is aware of deficiencies in detection and has commissioned a number of research projects to inform New South Wales' approach to cyber security.

Not all incidents are centrally reported which limits the ability to respond and contain

Requirements

- The Policy requires that digital information security events, incidents and near misses that pose a threat across the public sector must be disseminated through the Digital Information Security Community of Practice in a time and manner appropriate to the nature and magnitude of the threat.
- The Information Security Event Reporting Protocol requires agencies to alert the Information Security Community of Practice immediately on govdex and by email to DFSI. This alert should identify that an incident or event has occurred and include the senior responsible officer's assessment of its impact to NSW Government.

Reporting cyber security incidents centrally is important because it allows the possibility of a coordinated response from the NSW public sector. Agencies will not know if an incident has spread, or been contained, unless they know whether other agencies have been attacked. Incidents may also go undetected in agencies if they are not communicated, and the response is also likely to be suboptimal if advice is not circulated.

Despite the mandatory reporting requirements in the Policy and the protocol, agencies do not always report incidents to DFSI. Of the ten case study agencies, three are not covered by the Policy and not required to report i.e. two State owned corporations and a university. Some other agencies had reported some incidents but not others, and some agencies said they would not report if they had an incident. Only a few of our case study agencies said they would report incidents to DFSI, or seek its advice, and most saw little benefit in doing so.

There is currently little incentive for agencies to report incidents to DFSI and a low likelihood of sanctions if they do not report. None of the case study agencies' response procedures included a requirement to report incidents to DFSI. This points to an inability of DFSI to monitor the effectiveness of the Policy and reporting protocol. We also note that DFSI has not dedicated resources for this purpose.

From July 2015 to September 2017 there were only 93 events, alerts and incidents reported to the DFSI email inbox. These include a mix of alerts regarding potential threats, and potential and actual incidents. Although limited detail is provided for these 93 events reported, around 40 were incidents with the potential to cause damage.

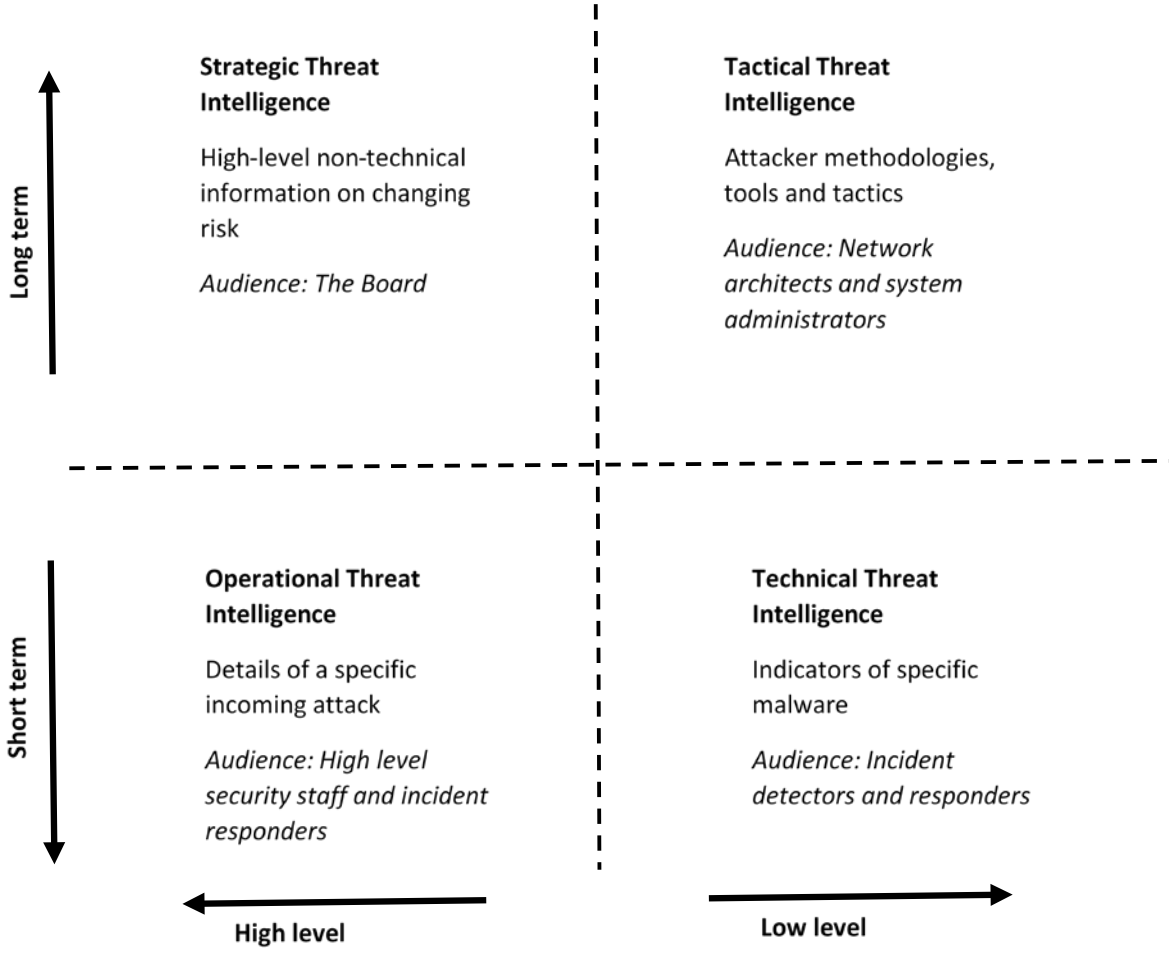
DFSI recognises that the Event Reporting Protocol needs updating to clearly describe what constitutes a reportable security event, and to provide a standardised reporting format and a single point of responsibility (outside of the Community of Practice) for receiving and acting on reports. This protocol should be able to be used by agencies of all sizes and complexity across the NSW public sector.

Intelligence gathering is limited

Currently gathering and sharing of threat intelligence at a whole-of-government level is ad hoc. DFSI has not allocated resources to gather intelligence and communicate it across government, although it has begun to build this capacity.

Any information about cyber threats that could inform decisions is arguably threat intelligence. Identifying types of threat intelligence can be based on who consumes the intelligence and what it aims to achieve.

Exhibit 5 – Types of threat intelligence



Source: MWR InfoSecurity, Information Security Whitepaper, 2015 / Audit Office 2017.

Most of the case study agencies rely on IT service providers for alerts regarding potential threats to their IT systems. Some agencies have also established informal links with cyber security organisations such as CERT Australia, the Australian Government computer emergency response team, and two have subscribed to AusCERT, a not-for-profit security group based at the University of Queensland, to assist in identifying imminent threats. Some links had also been established with other intelligence gathering agencies, such as the Australian Signals Directorate (ASD) and ASIO.

DFSI retains a contact list of senior officers in agencies that make up the Information Security Community of Practice (on the govdex website). Such a list should allow DFSI to contact agencies to notify of threats and incidents, however this list is not well maintained. For example, of our ten case study agencies, three did not have an officer listed in the contact list and the contact details for another three agencies were out-of-date. This means it may not be possible to effectively communicate imminent threats to the senior cyber security staff in over half of the case study agencies.

It is unclear how much support the NSW public sector can expect from Australian Government agencies during a major cyber security incident, especially if the incident also impacts Australian Government and private enterprise. There are no formal arrangements in place, at an agency or whole-of-government level, for agencies to be notified, advised or supported by Australian Government security agencies during an incident. There are also no reciprocal arrangements in place for support from other states.

The GCISO should work with other jurisdictions, including the Australian Government, other States and Territories, to identify how they can best support each other.

3.2 Barriers to whole-of-government incident response

No central coordination of response risks increased damage to multiple agencies

A lack of central coordination in incident response risks delays and increases the likelihood of incidents spreading to multiple agencies.

When incidents have been reported, DFSI has not provided dedicated resources to assess them and coordinate the public sector's response. DFSI's approach, until recently, has been limited to defining policy level requirements, bi-annual reporting on the implementation of an Information Security Management System (ISMS) for agencies; and providing limited coordination of threat and incident information between agencies.

There are no procedures to guide DFSI staff on what they should do if incidents are reported to them. There are currently no guidelines to assist the assessment of the incident and no official escalation process across whole-of-government. There are also no processes in place for the coordination of Ministerial briefings, media releases or public relations.

This means responsibilities for the overall coordination are unclear and there is no requirement for a whole-of-government team to alert and advise agencies under threat or the broader community. The 2016 survey of public sector agencies found that limited crisis management capabilities are in place to deal with a significant cyber event within certain clusters, and in the event that a crisis spans multiple clusters, there was limited planning in place for a coordinated cyber response.

One of the key accountabilities of the newly created GCISO role is to coordinate efforts to increase the NSW Government's ability to respond to and recover from threats and attacks, including investigations and recommendations after breaches or incidents. Although detailed plans and funding models are yet to be developed, the GCISO has developed a strategic cyber security roadmap which includes a range of possible initiatives to improve whole-of-government detection and response capabilities. These include improved threat and intelligence sharing, cyber culture and awareness programs and a whole-of-government security operations/coordination centre.

Central guidelines are weak on what to report and when, thereby limiting the value of information provided

Requirement

The Policy requires that digital information security events, incidents and near misses that pose a threat across the public sector must be disseminated in a time and manner appropriate to the nature and magnitude of the threat.

Some guidance is provided in the Policy on a range of aspects to consider when determining the nature of such a threat. However, no examples are provided on the types of incidents that need to be reported and when this should occur.

The information security protocol states that events are to be reported immediately on govdex (an online portal) and the DFSI incident email inbox, but goes on to state that 'senior responsible officers must only provide information once it has been de-sensitised to ensure there is no inappropriate disclosure of classified information.'

The Australian Government Information Security Manual specifies the types of incidents agencies should report to ASD, including:

- suspicious or seemingly targeted emails with attachments or links
- any compromise or corruption of information
- unauthorised access or intrusion into an ICT system
- data spills
- theft or loss of electronic devices that have processed or stored Australian Government information
- intentional or accidental introduction of viruses to a network
- denial of service attacks
- suspicious or unauthorised network activity.

The South Australian and Queensland cyber security incident reporting schemes also provide examples of incidents that should be reported, as well as examples of the types of events that don't need to be reported. In the South Australian scheme it also states: 'if in doubt, report it'.

DFSI plans to review the Digital Information Security Policy in line with the key objectives of the newly appointed GCISO. This should include strengthening the Policy to ensure effective cyber risk reporting.

No standard format for reporting makes it difficult to determine a response

There is currently no whole-of-government reporting template enabling agencies to report incidents in a consistent manner. This means that DFSI lacks the necessary information for adequately assessing an incident, including the level of risk associated with it, limiting its ability to respond to incidents and develop reliable statistics. Incidents could occur that impact the effectiveness of multiple agencies, or even government responsibility to the community, but the source agency may not be providing the details necessary for other agencies to respond effectively.

Requirement

The Information Security Event Reporting Protocol requires that every incident reported should include an assessment of its impact to NSW Government.

We expected to see a standardised method for reporting incidents, outlining the details required to adequately record and assess each incident. Such a system would make it easier for agencies to report incidents to DFSI and should make it is easier for DFSI to assess the incident and decide how to respond.

We selected a sample of incidents agencies have reported to DFSI since July 2017 to gauge the level of detail of reporting by agencies and follow-up by DFSI. Given that these were some of the more serious incidents, we expected to see a reasonable level of detail in reporting and some post-incident analysis.

We found that agencies' notifications to DFSI lacked detail and analysis. Information we expected to find but was not provided included:

- the start date of each incident
- where or who the attack came from
- the security vulnerability exploited
- the impact of the incident
- post-incident reports and lessons learnt.

The lack of this information limits DFSI's ability to gauge the full extent of possible impacts across NSW Government in terms of service delays, financial losses and adverse impacts on other parties.

The GCISO team advised that it is currently drafting procedures to improve the reporting of cyber incidents including:

- a template for use by agencies to report a cyber incident to the office of GCISO - to create comprehensive record of each incident that can be used to generate regular tracking and reporting to GCISO
- working to improve the frequency and timeliness of posting to govdex of information on cyber incidents from a whole-of-government perspective for all of Community of Practice members to access.

Limited avenues for sharing information after incidents are resolved

Currently there is ad hoc sharing of information on incidents at a whole-of-government level.

As previously discussed, not all incidents occurring in public sector agencies are reported to DFSI. When incidents are reported to DFSI, limited detail is provided to allow an assessment of the incident. Further, it is not clear how many agencies conducted a post-incident review as these are not provided to DFSI after each notification. There is also no evidence to indicate DFSI is made aware of the duration and the root cause of each incident and there is no standard template for such post-incident reviews. This lack of understanding limits DFSI's ability to communicate lessons learned to the rest of the public sector.

If the NSW public sector does not learn from incidents it may not be able to identify and implement the necessary preventative controls, and other corrective action, to limit the likelihood and impact of future incidents.

Some information on incidents is shared at the Information Security Community of Practice in-person forums held every two months of the year. However, only a few of our case study agencies indicated they had attended these meetings, as most saw little value in participating. Minutes are not taken at these meetings and attendance is not recorded, so we do not know whether the Community of Practice is an effective forum for knowledge sharing.

Some information sharing does occur via the Community of Practice online forum (on the govdex website), that includes information and some discussion on cyber security events and alerts, and some advice on how to manage them. However, members of the Information Security Steering Group (ISSG) recently agreed the generic nature of many govdex alerts did not assist Community of Practice members to assess potential risks and identify best-practice actions for their own agencies.

Some sharing also occurs amongst members at the ISSG which meets monthly, including some discussion on recent govdex alerts. A recent standing item on the ISSG agenda is for agency representatives to brief the group on any recent incidents.

Since the GCISO has been appointed, one whole-of-government post-incident review has been conducted and reported to the Secretaries' Board, which is made up of the secretaries from government departments and the Public Service Commissioner.

Section two

Appendices

Appendix one – Response from agency

Finance, Services & Innovation
NSW GOVERNMENT

McKell Building – 2-24 Rawson Place, Sydney NSW 2000
Tel 02 9372 8877 | TTY 1300 301 181
ABN 81 913 830 179 | www.finance.nsw.gov.au

Office of the Secretary

Our ref: DOC18/61923
Your ref: PA6603

Ms Margaret Crawford
Auditor-General of NSW
Audit Office of NSW

Via e-mail: margaret.crawford@audit.nsw.gov.au

Dear Ms Crawford Margaret

Thank you for your letter dated 8 February 2018 and the opportunity for the Department of Finance, Services and Innovation (DFSI) to respond to your final report of the performance audit – *detecting and responding to cyber security incidents*.

The report outlines current weaknesses in the NSW public sector's ability to detect and respond to incidents and highlights areas requiring improvement. DFSI is committed to ensuring a cyber safe NSW government. Following the appointment of the Government Chief Information Security Officer (GCISO) in May 2017, work has commenced to improve cyber security capability across the public sector. This includes coordinating efforts to increase the NSW Government's ability to respond to and recover from whole-of-government threats and attacks. Specifically, the GCISO is working collaboratively across clusters on:

- coordinated mandatory cyber event and incident reporting
- improved information sharing and advice
- cyber capability stocktake and uplift strategy
- whole-of-government cyber security standards
- post-incident reviews and improvement plans
- shared cyber security services
- integrated cyber security, and
- whole-of-government response plan.

DFSI agrees with the general findings and recommendations outlined in the report and it will provide further impetus for the GCISO to continue facilitating a collaborative approach to designing effective, integrated and sustainable cyber security prevention and response for NSW Government.

It should be noted that the response strategy cannot be achieved without investment in cyber security and so the findings and recommendations will be considered in the context of government funding priorities.

Yours sincerely

Martin Hoffman
Secretary

15 February 2018

Appendix two – ISMS maturity model

Public sector agencies are required to rate themselves from one to five against the following 12 'actions' as part of an Information Security Management System (ISMS) model. The risk matrix developed to assess this maturity is presented on the following page.

Action number	Action name
Action 1	ISMS governance is established and aligned to implementation of risk management policies.
Action 2	ISMS is reviewed in accordance to the level of risks to digital information and digital information system.
Action 3	All digital information is classified to ensure it is handled with appropriate level of protection under the NSW Government Information Classification and Labelling Guidelines.
Action 4	Access to digital information and digital information systems is monitored and controlled.
Action 5	Controls are in place and working effectively to prevent unauthorised disclosure, modification, removal or destruction of digital information.
Action 6	Security requirements are considered and implemented as part of the acquisition, development and maintenance of information systems and services.
Action 7	The security of digital information and digital information systems accessed, processed, communicated to, or managed by external parties is controlled.
Action 8	The security of digital information and software exchanged with external entities is maintained.
Action 9	Controls are in place to counteract interruptions to business activities and to ensure that IT systems support the recovery of critical business processes, and are tested at planned intervals.
Action 10	The timely resumption of business processes in the event of a major failure is ensured.
Action 11	Processes are in place for the communication of digital information security events and weaknesses associated with digital information systems within the agency and across the sector as appropriate.
Action 12	Awareness training program is implemented and maintained.

Matrix for agencies to assess their maturity scores

Key attributes					
Optimised	Information owners accountable Risk-aware culture Automated controls in place and corrective action integrated within process Continuous evaluation and improvement regular reviews of risks Benchmarking in place Policies and processes are providing auditable benefits By design solution incorporated in new assets	3	4	5
Managed	Governance body established Info-centric approach Security organisation working well Effective KPIs, metrics and reporting in place Controls implemented according to risk assessment Value is promoted	3	3	4
Defined	Policies and processes defined Security organisation defined Improving user awareness Risk assessment performed	2	3	3
Developing	CISO appointed Formal program(s) initiated User awareness initiated	1	2	2
Initiated	Ad hoc activities Loosely controlled and reactive Initial Executive Awareness Policies and process not defined or only partially defined	1	1	2
		1% – 33%	34% – 66%	67% – 100%
		Only high risk assets covered	Some of the existing assets/process/ system covered	Majority of existing assets/process /system covered

Appendix three – About the audit

Audit objective

This audit assessed how well cyber incidents are monitored and remedial advice is communicated in the NSW public sector.

Audit criteria

We addressed the audit objective with the following lines of inquiry:

1. Cyber security incidents are monitored efficiently and effectively
    a) Processes are in place for monitoring cyber incidents within and across agencies.
    b) Appropriate mechanisms are in place for agencies to report cyber incidents, including clear guidance on whom to report to
    c) Counter-intelligence on cyber incidents is shared between state and federal agencies, and the private sector.
2. Agencies receive timely and quality advice on cyber incidents and remedial action
    a) Incidents are assessed and a suitable response determined
    b) Agencies under threat are notified
    c) Advice on remedial action is provided from internal and/or external sources.

Audit scope and focus

In assessing the criteria, we checked the following aspects:

1. Incidents that have taken place since July 2015
2. Interviews with relevant staff in DFSI and the case-study agencies
3. Interviews with Australian Government agencies involved in coordinating cyber security
4. Review of documents on the relevant policies and procedures for detecting, monitoring and communicated cyber-events.

This audit focused on the following three areas:

1. Monitoring and detection of cyber incidents
2. Reporting and communication about cyber incidents
3. The communication of advice on remedial action.

A cyber incident, for the purposes of this audit, is a past or ongoing intrusion, disruption, or other event that impairs the confidentiality, integrity, or availability of electronic information, information systems, services, or networks. Cyber incidents include major events impacting other jurisdictions, even if they do not directly impact NSW public sector agencies or universities.

Audit exclusions

The audit did not:

- Conduct a technical analysis on the adequacy of processes agencies used to detect and respond to cyber incidents
- Examine the controls agencies use to prevent cyber security incidents
- Analyse the quality of technical advice provided to agencies
- Question the merits of government policy objectives.

Audit approach

Our procedures included:

1. Interviewing relevant staff involved in detecting cyber security incidents, reporting cyber security incidents and, sharing information about cyber security incidents in the agencies.

2. Examining
    a) Procedures and processes for detecting and responding to cyber security incidents
    b) Information on cyber incidents reported since July 2016
    c) Procedures for gathering and sharing counter-intelligence information including communications with other government agencies, NGOs and the private sector.

The audit approach was complemented by quality assurance processes within the Audit Office to ensure compliance with professional standards and technical advice from an expert consultant.

Audit methodology

Our performance audit methodology is designed to satisfy Australian Audit Standards ASAE 3500 on performance auditing. The Standard requires the audit team to comply with relevant ethical requirements and plan and perform the audit to obtain reasonable assurance and draw a conclusion on the audit objective. Our processes have also been designed to comply with the auditing requirements specified in the *Public Finance and Audit Act 1983*.

Acknowledgements

We gratefully acknowledge the cooperation and assistance provided by the Department of Finance, Services and Innovation and all of the case study agencies. In particular, we wish to thank our liaison officers and staff who participated in interviews and provided material relevant to the audit.

We would also like to thank other stakeholders that spoke to us and provided material during the audit.

Audit cost

Including staff costs, travel and overheads, the estimated cost of the audit is $348,342.

Appendix four – Performance auditing

What are performance audits?

Performance audits determine whether an agency is carrying out its activities effectively, and doing so economically and efficiently and in compliance with all relevant laws.

The activities examined by a performance audit may include a government program, all or part of a government agency or consider particular issues which affect the whole public sector. They cannot question the merits of government policy objectives.

The Auditor-General's mandate to undertake performance audits is set out in section 38B of the *Public Finance and Audit Act 1983*.

Why do we conduct performance audits?

Performance audits provide independent assurance to parliament and the public.

Through their recommendations, performance audits seek to improve the efficiency and effectiveness of government agencies so that the community receives value for money from government services.

Performance audits also focus on assisting accountability processes by holding managers to account for agency performance.

Performance audits are selected at the discretion of the Auditor-General who seeks input from parliamentarians, the public, agencies and Audit Office research.

How are performance audits selected

When selecting and scoping topics, we aim to choose topics that reflect the interests of parliament in holding the government to account. Performance audits are selected at the discretion of the Auditor-General based on our own research, suggestions from the public, and consultation with parliamentarians, agency heads and key government stakeholders. Our three-year performance audit program is published on the website and is reviewed annually to ensure it continues to address significant issues of interest to parliament, aligns with government priorities, and reflects contemporary thinking on public sector management. Our program is sufficiently flexible to allow us to respond readily to any emerging issues.

What happens during the phases of a performance audit?

Performance audits have three key phases: planning, fieldwork and report writing. They can take up to nine months to complete, depending on the audit's scope.

During the planning phase the audit team develops an understanding of agency activities and defines the objective and scope of the audit.

The planning phase also identifies the audit criteria. These are standards of performance against which the agency or program activities are assessed. Criteria may be based on best practice, government targets, benchmarks or published guidelines.

At the completion of fieldwork the audit team meets with agency management to discuss all significant matters arising out of the audit. Following this, a draft performance audit report is prepared.

The audit team then meets with agency management to check that facts presented in the draft report are accurate and that recommendations are practical and appropriate.

A final report is then provided to the agency head for comment. The relevant minister and the Treasurer are also provided with a copy of the final report. The report tabled in parliament includes a response from the agency head on the report's conclusion and recommendations. In multiple agency performance audits there may be responses from more than one agency or from a nominated coordinating agency.

Do we check to see if recommendations have been implemented?

Following the tabling of the report in parliament, agencies are requested to advise the Audit Office on action taken, or proposed, against each of the report's recommendations. It is usual for agency audit committees to monitor progress with the implementation of recommendations.

In addition, it is the practice of Parliament's Public Accounts Committee (PAC) to conduct reviews or hold inquiries into matters raised in performance audit reports. The reviews and inquiries are usually held 12 months after the report is tabled. These reports are available on the parliamentary website.

Who audits the auditors?

Our performance audits are subject to internal and external quality reviews against relevant Australian and international standards.

Internal quality control review of each audit ensures compliance with Australian assurance standards. Periodic review by other Audit Offices tests our activities against best practice.

The PAC is also responsible for overseeing the performance of the Audit Office and conducts a review of our operations every four years. The review's report is tabled in parliament and available on its website.

Who pays for performance audits?

No fee is charged for performance audits. Our performance audit services are funded by the NSW Parliament.

Further information and copies of reports

For further information, including copies of performance audit reports and a list of audits currently in progress, please see our website www.audit.nsw.gov.au or contact us on 9275 7100.

Professional people with purpose

OUR VISION

Our insights inform and challenge government to improve outcomes for citizens.

OUR PURPOSE

To help parliament hold government accountable for its use of public resources.

OUR VALUES

Purpose – we have an impact, are accountable, and work as a team.

People – we trust and respect others and have a balanced approach to work.

Professionalism – we are recognised for our independence and integrity and the value we deliver.

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au

Level 15, 1 Margaret Street
Sydney NSW 2000 Australia

PHONE +61 2 9275 7100
FAX +61 2 9275 7200

mail@audit.nsw.gov.au

Office hours: 8.30am-5.00pm,
Monday to Friday.

auditoffice
OF NEW SOUTH WALES

audit.nsw.gov.au