7.2. Reporting Information Security Incidents

Objective

7.2.1. Reporting of information security incidents is incorporated as an essential part of incident management, whether the reporting is within an agency or reports are provided to another government agency.

7.2.2. Reporting helps to maintain an accurate threat environment picture for government systems, particularly when All-of-Government (AoG) or multi-agency systems are involved.

Context

Scope

7.2.3. This section covers information relating specifically to the reporting of information security incidents. It does **not** cover the reporting of physical or personnel security incidents **unless** there is an impact on information systems.
For example, keypads and access cards are part of a wider information technology system, where physical key locks are not.

7.2.4. It is important to note that, in most cases, information systems are likely to be affected.

Requirement for information security incident reporting

7.2.5. The requirement to report an information security incident report applies irrespective of whether incident management is internally managed or if an agency has outsourced some or all of its information technology functions and services.

7.2.6. The information security threat and intelligence landscape continues to evolve, partly driven by more advanced, capable, well-resourced and motivated adversaries, as well as the need to improve management and governance of information systems. To assist in managing these requirements, a standardised form of information exchange is essential.

7.2.7. Agencies must have a comprehensive understanding of their assets, both physical and intellectual. By establishing clear boundaries, they can effectively manage their scope, ensuring informed decisions and efficient incident response.

7.2.8. Agencies need to consider that vendor contract(s) and agreement(s) enable sharing of information relating to incidents with the NCSC.

Definition of a Security Incident

7.2.9. A **security incident** is a violation, breach or infringement of a security policy or an attempt to gain unauthorised access to official resources. It is important to note that security incidents include physical incidents (such as lost documents) as well as “cyber” incidents.

Definition of a Cyber Security Incident

7.2.10. A **cyber security incident** is any event that jeopardises or may jeopardise the confidentiality, integrity, or availability of an information system or the information a system processes, stores, or communicates. This includes a violation or potential violation of security policies, security procedures, acceptable use policies or any relevant regulation or legislation.

Background

7.2.11. The detection, triaging, recording, management and response to an incident depends primarily on effective prevention and detection mechanisms and a robust response plan. Effective detection and response mechanisms also provide an important record of events and assist in preventing repeat events, improving defences and streamlining response measures.

7.2.12. A key part of the detection and response is incident reporting, including internal security system reports as well as any essential external reporting. It is essential that response is timely and methodical in order to minimise the effects of the incident. In all cases it is vital that steps are taken to quickly contain the incident, minimise damage and implement measures to prevent or contain any reoccurrence.

7.2.13. Not every cybersecurity event is serious enough to warrant detailed investigation and reporting, for example a single multi-factor authentication challenge failure from an employee on premises. Multiple multi-factor challenge failures, however, may indicate a malicious access attempt. Thresholds should be established which will trigger an incident response. In all cases, once an incident has been determined, it should be recorded to support analysis and reporting.

7.2.14. It is also important to categorise incidents in order to better manage allocation of resources to the containment and remediation of the incident. A three-tier categorisation is suggested:

1. **Critical**: Incident affecting critical systems or information with potential to impact operations, revenue, customers or information disclosed in data breach.
   For example, distributed denial of service attack, unauthorised access to system, multi-system ransomware.

2. **Serious**: Incident affecting noncritical systems or information, impact on operations, revenue, customers or information disclosed in data breach.
   For example, execution of malware on a single system, potentially compromised credentials.

3. **Low**: Possible incident affecting noncritical systems. Incidents or employee investigations that are not time sensitive.
   For example, blocked phishing attempts.

7.2.15. Incidents where the scope or cause of activity has not yet been determined should be categorised as serious or critical and actioned accordingly.

7.2.16. Factors that assist in determining the severity of an incident include:

- Whether the incident affects a single agency or multiple agencies;
- Functional impact of the incident (availability);
- Information impact of the incident (confidentiality, integrity);
- Recoverability from the incident;
- Whether a breach of personal information held by the agency has occurred;
- Whether unauthorised access to agency information systems may have occurred;
- Reputational risk to the agency;
- Impact on any MOUs, MOAs and similar formal agreements;
- Impact on the disclosure of information theft of data.

References

7.2.17. Additional information relating to information security incidents can be found at:

Reference	Title	Publisher	Source
SP 800-61r3 April 2025	**Computer Security Incident Handling Guide,**	**NIST**	**Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile**
SP 800-60 Volume 1 Revision 1	**Guide for Mapping Types of Information and Information Systems to Security Categories**	NIST	SP 800-60 Vol. 1 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories | CSRC
SP 800-60 Volume 2 Revision 1	**Guide for Mapping Types of Information and Information Systems to Security Categories, Volume ll: Appendices**	NIST	SP 800-60 Vol. 2 Rev. 1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices | CSRC
	Guide to cyber threat sharing	NIST	Guide to cyber threat sharing
	Cyber Threats and Advisories	CISA	Cyber Threats and Advisories | Cybersecurity and Infrastructure Security Agency CISA

Rationale & Controls

Reporting information security incidents

7.2.18.R.01. **Rationale**

Reporting information security incidents provides management with a means to assess and minimise damage to a system and to take remedial actions. Incidents should be reported to an ITSM, as soon as possible. The ITSM or CISO may seek advice from NCSC as required.

7.2.18.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1203]

Agencies MUST direct personnel to report information security incidents to an ITSM as soon as possible after the information security incident is discovered in accordance with agency procedures.

7.2.18.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1205]

Agencies SHOULD:

- encourage personnel to note and report any observed or suspected security weaknesses in, or threats to, systems or services;
- establish and follow procedures for reporting system, software or other malfunctions;
- put mechanisms in place to enable the types, volumes and costs of information security incidents and malfunctions to be quantified and monitored; and
- deal with the violation of agency information security policies and procedures by personnel through training and, where warranted, a formal disciplinary process.

Responsibilities when reporting an information security incident

7.2.19.R.01. **Rationale**

The ITSM actively manages information security incidents and MUST ensure the CISO has sufficient awareness of and information on any information security incidents within an agency.

The CISO is required to keep the CSO and/or Agency Head informed of information security incidents within their agency.

7.2.19.R.02. **Rationale**

Reporting on Critical and Serious incidents requires immediate action.

Reporting on incidents categorised as Low can usually be adequately managed through periodic (weekly or monthly) reports.

7.2.19.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1211]

The ITSM MUST keep the CISO fully informed of information security incidents within an agency.

Reporting information security incidents to National Cyber Security Centre (NCSC)

7.2.20.R.01. **Rationale**

The NCSC uses significant information security incident reports as the basis for identifying and responding to information security events across government, and New Zealand. Reports are also used to develop new policy, procedures, techniques and training measures to prevent the recurrence of similar information security incidents across government.

7.2.20.R.02. **Rationale**

Reporting on Critical and Serious incidents requires immediate action.

Reporting of Critical or Serious information security incidents to the NCSC through the appropriate channels ensures that appropriate and timely assistance can be provided to the agency. In addition, it allows the NCSC to maintain an accurate threat environment view across government systems.

7.2.20.R.03. **Rationale**

Reporting on incidents categorised as Low can be scheduled to a suitable timeframe e.g. weekly.

7.2.20.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1216]

The Agency ITSM, MUST report information security incidents categorised as:

- **Critical**;
- **Serious**; or
- incidents related to multi-agency or government systems;

to the NCSC as soon as possible.

A Report Form is provided on the NCSC website under Reporting an Incident at Report an incident and request support | National Cyber Security Centre

7.2.20.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1220]

Agencies SHOULD report information security incidents categorised as **Low** to the NCSC.

A Report Form is provided on the NCSC website under Reporting an Incident at Report an incident and request support | National Cyber Security Centre

7.2.20.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7536]

Agencies SHOULD formally share post-incident review reports by emailing them to incidents@ncsc.govt.nz.

Outsourcing and information security incidents

7.2.21.R.01. **Rationale**

In the case of outsourcing of information technology services and functions, the agency remains responsible for the reporting of all information security incidents. This includes any outsourced cloud services used by the agency. As such, the agency MUST ensure that the service provider informs them of all information security incidents to enable them to assess the incident and provide formal reporting.

7.2.21.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1226]

Agencies that outsource their information technology services and functions MUST ensure that the service provider advises and consults with the agency when an information security incident occurs.

Cryptographic keying material

7.2.22.R.01. **Rationale**

Reporting any information security incident involving the loss or misuse of cryptographic keying material is particularly important. Systems users in this situation are those that rely on the use of cryptographic keying material for the confidentiality and integrity of their secure communications.

7.2.22.R.02. **Rationale**

It is important to note that a loss or compromise of keying material is a Critical or Serious information security incident and strict procedures must be followed to minimise the impact of the incident.

7.2.22.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1233]

Agencies MUST notify all system users of any suspected or confirmed loss or compromise of keying material.

Replacement of Cryptographic Key (HACE) keying material

7.2.23.R.01. **Rationale**

If an encryption key is compromised, there is no need to attack the algorithm itself and it is a trivial matter to decrypt any encrypted data. This is why strong key management is vital in order to protect the encryption keying materials. If a compromise of keying materials is known or even suspected, the cryptographic key must be replaced as a matter of urgency and measures taken to reduce the impact of the key compromise. See also Section 17.9 – Key Management.

7.2.23.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:6592]

Agencies MUST replace compromised cryptographic keys as a matter of urgency and record the replacement in the incident reporting.

High Assurance Cryptographic Equipment (HACE) keying material

7.2.24.R.01. **Rationale**

For information security incidents involving the suspected loss or compromise of HACE keying material, GCSB will investigate the possibility of compromise, and where possible, initiate action to reduce the impact of the compromise.

7.2.24.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1237]

Agencies MUST urgently notify GCSB of any suspected loss or compromise of keying material associated with HACE.