National Cyber
Security Centre
a part of GCHQ

Cyber Incident Response Standard (Level 1)

Version 1.1 (January 2022)

Contents

1. Definitions used in this document 3

2. Scope 5

3. Core competencies 6

5. Use of applied TI 7

6. Communication requirements 8

7. Staff requirements 10

8. Scope of work 12

9. Technical capabilities for incident investigation 13

10. Reporting and interaction with external stakeholders 17

11. Retainer model 19

Appendix A: Example scope of work 20

Appendix B: Evidence required 21

1. Definitions used in this document

Attacker

1. Malicious actor who seeks to exploit computer systems with the intent to change, destroy, steal or disable their information, and then exploit the outcome.

CIR

2. Cyber Incident Response. The activities which take place during and immediately after a cyber incident response, such as determining the extent of an incident, managing its impact, restoring systems, and working to increase security across the network.

CIR Provider

3. The company providing the cyber incident response (CIR) service.

Common Legacy Operating Systems

4. Any version of Windows, MacOS or Linux for which vendor support ended in the previous 5 years.

Common Supported Mobile Operating Systems

5. Any version of Android or iOS which is currently supported by the developer.

Common Supported Operating Systems

6. Any version of Windows, MacOS or Linux which is currently supported by the developer.

Engaged

7. A Target Organisation is engaged by a CIR Provider at the point at which a contract has been signed in support of an initial scope of work.

Endpoint Detection and Response (EDR)

8. Activities focussed on detecting and investigating suspicious activities and other problems on end-user devices such as workstations, laptops and smartphones.

MITRE ATT&CK

9. MITRE ATT&CK is a knowledge base of adversary tactics and techniques used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cyber security community.

STiX v2.1

10. Structured Threat Information Expression (STIX™) is a language and serialisation format used to exchange cyber TI.

TTPs

11. The Tactics, Techniques and Procedures of an attacker. Patterns of activities or methods associated with a specific threat actor or group of threat actors.

Target Organisation

12. The organisation that is a consumer of the CIR service.

Threat Intelligence (TI)

13. Threat Intelligence. Information about threats that has been aggregated, analysed and enriched to provide the useful context for decision-making processes.

Unusual Operating Systems

14. Any non-mobile operating system not covered by the definitions of:

    a. common supported operating systems

    b. common legacy operating systems

    c. common supported mobile operating systems

2. Scope

15. Incident Response takes place during and immediately after a cyber incident. This document sets out the standards which current and prospective CIR Providers are assessed against, in order to become an NCSC-assured CIR Provider. It defines the expected range of cyber crisis management assistance of an incident for Target Organisations dealing with category 1, category 2, and category 3 incidents, as defined by the NCSC's cyber attack categorisation system.

16. The CIR Provider may be expected to be able to take over full control of an incident for the Target Organisation (or to step in at any point of an incident), so the scope of work may be altered throughout the project (dependent on the contractual agreement and severity of the incident).

17. The requirements described below provide clear and concise instructions for current and new CIR Providers to follow, in order to submit and retain their status as an accredited CIR Provider.

Exclusions

18. The work of the CIR Provider is always in accordance with the instructions of the Target Organisation. The CIR Provider is expected to advise the Target Organisation, but if the Target Organisation decides not to take the advice (or that they do not wish the CIR Provider to undertake certain activities) then there will be no negative consequence in the assessment of the CIR Provider against this standard.

3. Core competencies

19. Incident response and management must be a core business function of the CIR Provider. CIR Providers should be capable of supporting a Target Organisation (where requested) to eradicate an attacker, secure their environment, help rebuild affected systems, and perform root cause analysis of how the incident occurred (where possible).

20. The CIR Provider must be able to provide evidence that proves they can:

    a. manage sophisticated cyber incidents occurring at any time (subject to reasonable capacity constraints cased by simultaneous incidents requiring response)

    b. manage multiple incidents (potentially across multiple Target Organisation) simultaneously

    c. provide experience of working with high profile and complex incidents

21. In practice this means providing evidence of how responses to incidents can be scaled across regions and include cross-discipline expertise (such as crisis management expertise), and an awareness of how legal considerations may impact a Target Organisation's response to an incident. This could be either as a direct part of the CIR team, or through working with other organisations with relevant expertise, or other CIR Providers.

22. The CIR Provider must be able to demonstrate its methodology and processes to the NCSC. Simply having access to skilled analysts is not sufficient; they must operate within a mature structure around a repeatable methodology. A formal written submission will be assessed first, followed by an oral assessment with the Head Consultant.

23. In addition, CIR Providers must be able to:

    a. Take over full control of an incident for the Target Organisation at any point of an incident with the ability to engage directly with the C-suite of a large company (e.g. FTSE 100) and suggest actions to take. Note: risk decisions would still be expected to lie with the customer, but the CIR should be capable of advising at this level and all levels below C-Suite.

    b. Provide a concise summary of a previous engagements in response to a sophisticated targeted attack. The summary should cover the full lifecycle of the engagement, including how the understanding of the capabilities of the attacker were analysed and used.

    c. Clearly demonstrate the use of appropriate analysis methods and selection of appropriate tools to support the analysis to provide an effective response to sophisticated attacks.

5. Use of applied TI

24. CIR Providers must make use of Threat Intelligence that they gather as part of their day-to-day operations (ie outside of incidents), during incident response in order to enhance the management of the incident.

Outside of incidents

25. The CIR Provider must generate their own Threat Intelligence. Information can be shared within the industry, but the CIR Provider should not rely wholly on third party Threat Intelligence. The CIR company may acquire Threat Intelligence from various sources, including publicly accessible intelligence, internal tools and techniques or using licensed Threat Intelligence platforms.

26. The CIR Provider must be able to represent their information in common formats for interchange with other organisations.

27. Overall Structured Threat Intelligence must be able to be represented as STiX v2.1.

28. TTPs must be mapped to MITRE ATT&CK where ATT&CK contains the TTPs in question.

29. CIR Providers must be able to generate SIGMA rules for host detection.

30. CIR Providers must be able to generate SNORT rules for network detection.

31. CIR Providers must be able to generate YARA Signatures for file and memory artefact identification.

Within incidents

32. CIR Providers must be able to demonstrate how Threat Intelligence is applied to the benefit of the Target Organisation, sharing this information with the Target Organisation where appropriate.

33. Threat Intelligence generated from an incident may be used after the incident for further analysis or for public consumption (either through anonymising the data or consent of the Target Organisation).

34. The intelligence should be used over the lifecycle of an incident. This may include assisting in the investigation of the incident, suggesting targets and motivations of the attacker, and predicting likely next steps by the attacker.

35. CIR Providers should be able to present information from Threat Intelligence to all levels within the Target Organisation.

6. Communication requirements

36. The CIR Provider must be able to demonstrate how it can communicate effectively across all levels within the Target Organisation, whether that’s board level, managerial level or operational level.

37. The CIR Provider must be able to communicate effectively to all stakeholders, including external stakeholders where appropriate.

38. The CIR Provider must have a Head Consultant who meets the requirements set out below. The Head Consultant will be accountable for the incident response services offered by the CIR Provider. The Head Consultant is responsible for ensuring that all work is delivered to a high standard, and for the overall quality of the technical output of a service offering. Work may be carried out by a team with a range of professional skills and experience.

39. The CIR Provider must capture and record every step of the incident including actions, findings and recommendations. The CIR Provider must have a repeatable methodology for capturing findings and recording decisions.

40. The CIR Provider's reports must be written in such a way that they can be widely understood across the Target Organisation. When jargon, technical wording or company-specific words are used, there must be glossary or ability to consult with the CIR Provider.

41. The CIR Provider should have a member of staff attached to the NCSC through the i100 scheme.

Board-level communications

42. The Cyber Incident Response Provider should be aware of the NCSC's Incident Management Guidance and the NCSC's Board Toolkit. CIR Providers must comply with the NCSC guidance unless there is an over-riding reason not to, in which case they will explain why they are diverging from the NCSC's guidance.

43. The CIR Provider may be engaged after the incident has occurred, so must be able to adapt to offer the most appropriate guidance and services for the situation the Target Organisation is in at the time of the engagement.

44. The CIR Provider must be able to engage with board-level executives on various topics, including but not limited to:

    - internal/external communications during an incident
    - helping the board to interpret and evaluate operational/technical reports
    - legal implications of the incident
    - all stages of an incident lifecycle as stated by the NIST Computer Security Incident Handling Guide (PDF)

45. When specified by the Target Organisation, the CIR Provider must have a dedicated member of staff that can communicate directly with a key contact within the board of the Target Organisation. This key contact will usually be the Target Organisation's CISO. If the Target Organisation does not have a formal CISO, it will be someone with equivalent responsibility, acting as the lead stakeholder for the incident on the Target Organisation side.

46. Where there are no technical contacts available, the CIR Provider should be able to manage a board level discussion, or train a board member (or equivalent) so they can assume this role. Though the CIR Provider is accountable for the response and deliverables, the board is the overall risk owner of the incident.

Stakeholder communications

47. The CIR Provider must obtain a contact list for all relevant external stakeholders, such as government and law enforcement, as well as all relevant internal stakeholders in the following areas for the incident response:
    - senior/executive management
    - incident manager
    - technical lead/recovery manager
    - crisis management, business continuity, disaster recovery
    - investigators and analysts, cyber security specialists
    - IT and infrastructure
    - other departments including legal, PR, HR and customer services
48. The CIR Provider does not need to be responsible for all elements of the response plan, it must ensure that lines of responsibility are clear and recorded.
49. The CIR Provider must offer 24/7 contact to the Target Organisation during an incident (can be via on-call arrangements).

7. Staff requirements

50. The CIR Provider must be able to offer a diverse technical skill set at all managerial and operational levels (including board level), so that these capabilities can be acted on accordingly and with competence. CIR Provider staff must have the relevant experience with appropriate qualifications, as described below.

51. At least one senior member of staff within the Cyber Incident Response Provider (such as a Head Consultant) must hold a Developed Vetting (DV) clearance. The NCSC will sponsor up to two DVs per Cyber Incident Response Provider in order to provide some contingency in case one member of staff leaves. The NCSC will accept a company without a DV while the DV request is being processed, if the company meet other onboarding requirements and technical assessment.

52. The CIR Provider must be able to deploy team members to identified locations to support the Target Organisation. CIR Providers are expected to be able to initiate deploying relevant staff globally within one working day of being engaged by a Target Organisation.

53. The CIR Provider must have a Head Consultant who has overall responsibility for the incident response services on their behalf. The Head Consultant must meet and maintain all of the relevant professional requirements whilst Engaged.

Head Consultant requirements

54. CIR Providers must have a Head Consultant who is accountable for the technical execution of the incident response services offered by the CIR provider.

55. Whilst the Head Consultant is unlikely to personally deliver all aspects of the incident response services offered by the CIR Provider, they are accountable for ensuring that it is delivered to a high standard, and for the overall quality of the technical output of the incident response.

56. The Head Consultant is accountable for ensuring that the following activities take place:

    a. identifying and fulfilling Target Organisation requirements with regard to the incident response

    b. ensuring that individuals assigned to a task have the appropriate technical competency

    c. maintaining effective communication channels with the Target Organisation, and all other interested parties

    d. reporting to the Target Organisation at regular intervals on progress or, as necessary, applying for further instructions or approval to proceed

    e. escalating any risks or issues to the board as appropriate

    f. knowledge transfer to other individuals within the Target Organisation

Professional requirements for the Head Consultant

57. A Head Consultant must be able to prove foundational knowledge of cyber security. This can be demonstrated through academic qualifications, professional certifications, or professional memberships. The following currently satisfy the requirements for proof of foundational knowledge (this list may be expanded, if additional proposals for inclusion provide a sufficiently broad and formally validated level of cyber security knowledge):

    a. an NCSC-certified degree (undergraduate or postgraduate)

    b. Certified Information Systems Security Professional (CISSP), including full membership of (ISC)

    c. Certified Information Security Manager (CISM), including full membership of ISACA

    d. full membership of the Chartered Institute for Information Security (CIISec)

    e. five years experience as a Senior Consultant in Cyber Incident Response

58. The Head Consultant will be required to demonstrate evidence of one of the above, typically through the submission of a valid and up-to-date certificate or other proof as appropriate.

59. Please contact the NCSC at CIR@ncsc.gov.uk to propose alternative professional certifications for consideration. As a guide, proposed professional certifications should:

    a. be directly applicable to the provision of incident response services

    b. be vendor neutral

    c. require an examination

    d. require evidence of professional practice

    e. require continued learning, or periodic recertification

60. Awards which are no longer valid, or associate membership of professional bodies in lieu of professional certifications will not be considered.

61. Where requested by the NCSC, the Head Consultant must be able to provide evidence, acceptable to the NCSC, which covers the work that they have conducted for customers in the context of Cyber Incident Response. This evidence may form part of the oral assessment referred to in paragraph 22 of this Standard.

8. Scope of work

62. As the scope of work is liable to change during an engagement, all versions of the scope of work must be retained. This will allow both providers and Target Organisations to see what work was agreed, and to assess the standard of the completed work.

63. As part of the audit process, the NCSC may investigate complaints made against a CIR provider. The Scope of Work is critical in enabling the NCSC to assess whether the CIR provider has completed the work as agreed.

64. An example scope of work is given in Appendix A.

65. Throughout the incident, the scope may be altered if both parties have agreed and the amendment has been logged. The CIR Provider must explain possible overlap between handovers or out of scope activities, to ensure the Target Organisation is aware of further issues.

66. For example, suppose the CIR Provider finds an indicator of compromise, and only shows the Target Organisation how it caused the incident. If the identification stage is all that is included within the statement of work, the Target Organisation may not be aware of the extent of how to mitigate the incident. The CIR Provider - in good faith - should at least offer an overlap, or clearly define the workload parameters. Allowing the Target Organisation the freedom to choose if the CIR Provider should amend their original scope of work to continue, or take matters into their own hands.

67. The CIR Provider staff should have experience of working with multi-nationals and across national borders and legal systems. CIR Providers are expected to operate only in countries where they fully understand applicable local laws.

9. Technical capabilities for incident investigation

68. The CIR Provider must have a broad range of capabilities to mitigate the incident at all levels, ranging from a mass data breach from an Advanced Persistent Threat (APT) on the network, to a member of staff losing a piece of equipment containing sensitive information. CIR Providers are not expected to necessarily have the level of staffing required to actually make changes to a Target Organisation's IT estate, but must be able to advise on containing or eradicating an incident, and on recovery to 'business as usual'. The CIR Provider should be able to support a handover (or offer flexibility to adjust the work package) and to extend the scope of work to assist in post incident recovery.

69. Note that CIR Providers are not mandated to use all the capabilities in this section for every Target Organisation in every incident. CIR Providers must have the ability to deploy these capabilities in the timeframes noted and the capabilities must fulfil the technical requirements, but it is not mandatory to deploy these capabilities unless required. The CIR Provider must have the ability to carry out actions to meet the Target Organisation's needs at agreed times (including out of hours), and should be able to demonstrate supplier SLAs and/or staff availability to support this.

Tooling agnostic

70. Although the CIR Provider must maintain the technical capabilities outlined below (so they can be immediately deployed to a Target Organisation's estate to inform threat hunting and incident scoping/remediation), they must also be ready to perform these tasks using a Target Organisation's existing tooling, should this be found to be technically sufficient.

71. A CIR Provider may recommend deploying replacement tools if the Target Organisation's capability is found to be lacking, but critically they should not be tied to their own tools or software if sufficient tooling is already present.

72. If replacement tools are recommended to be deployed then the CIR Provider must explain the reasoning for the replacement.

Endpoint Detection and Response (EDR)

73. The CIR Provider must have the capability to be able to deploy EDR capability rapidly to gain visibility of hosts, running Common Supported Operating Systems.

74. Provided Target Organisations can meet the necessary requirements to enable the deployment, the CIR Provider must be able to be provide EDR deployment resources (such as installation software) within 24 hours of engagement. A CIR Provider will not be adversely assessed against the standard if the speed of deployment is affected by issues which the Target Organisation is responsible for (such as their own staff or Managed Service Provider not being resourced to deploy software at scale).

75. EDR tools may be developed in house, or may be licensed by the CIR Provider from a third party.

76. CIR Providers' EDR suite(s) must be capable of being used by Common Supported Operating Systems, and should support at least one major version earlier. The CIR Provider must be able to explain the impact of deploying the EDR including any known compatibility issues and load on devices or network bandwidth etc.

77. EDR deployment must be supported by personnel who may (or may not) be direct employees of the CIR Provider. Where the support personnel are not direct employees, the CIR Provider is responsible for their performance in accordance with clause 24.1 of the Agreement and must ensure that there is a proper agreement with external personnel to cover 24/7 support of the EDR while deployed.

78. A full technical overview of the EDR capability service must be offered to the Target Organisation, so that they are fully aware of the implications and course of action from release to clean up. The technology should have minimal footprint on the operational tasks of the devices, but still return practical data or control; it is the Target Organisation's decision to use the tool or not.

79. CIR Providers must have the capability to effectively gain visibility on the Target Organisation systems and so EDR suites deployed must support:

    a. near real-time collection of process creation, network activity and system changes

    b. collection of artefacts such as files and system memory

    c. searching for files that match known signatures

80. EDR products can support other functionality such as response actions on end points to block or remove attacker activity.

Log collection and analysis

81. The CIR Provider must be capable of assisting in log collection at scale.

82. The CIR Provider must be capable of performing log analysis for large, heterogeneous estates, and include both on-premise and cloud systems.

83. Provided Target Organisations can meet the necessary requirements to enable the deployment, the CIR Provider must be able to be deploy a log collection system to a Target Organisation within 24 hours of being formally Engaged.

84. The CIR Provider must be able to ensure data feeds into the log collection system as soon as the Target Organisation can provide this.

85. The CIR Provider must have proven experience of log analysis on any scale.

86. CIR Providers must be able to demonstrate maturity in log analysis approach; that is, the ability to clean, transform, process, and ingest log sources to appropriate investigation environments. This should include basic understanding of statistical analysis techniques and methods to build statistics and insight from large data sets.

Network traffic inspection

87. The CIR Provider must be able to deploy network traffic inspection capability rapidly to gain visibility of network activity.

88. The CIR Provider must be capable of commencing deployment of network capture equipment to a Target Organisation site within 24 hours of formal engagement.

89. The CIR Provider must be able to identify anomalies, malicious activity which may have been involved in an incident.

90. The CIR Provider must be able to work with the Target Organisation to identify where to deploy network inspection tooling.

91. The CIR Provider's Network traffic inspection capability must be able to collect full packet captures, network flow information and/or identify packets that match pre-defined signatures. Which (if any) of these capabilities is required in a specific Incident is up to the CIR Provider's discretion.

Digital investigation/analysis

92. The CIR Provider must be capable of host forensics, encompassing artefact analysis, on-host historic log analysis and full disk forensics, on Common Supported Operating Systems.

93. Under all circumstances, the CIR Provider must conduct forensic analysis in a structured way which, if necessary, could be presented in a court of law in any relevant jurisdiction (for example, following the spirit of the ACPO Good Practice Guide [PDF] for the UK, noting that the actual guide is slightly outdated).

94. Incident responders from the CIR Provider could be deployed to the local area to start forensic duties. This must be carried out with the authority and permission of the Target Organisation. Other legal and regulatory restrictions may also need to be considered in any digital forensics work (such as data protection law, prohibitions on unlawful interception, rules of evidence and computer misuse prohibitions). CIR Provider staff must be trained to handle, capture and document evidence according to appropriate industry guidelines, such as the ACPO principles. CIR Providers should also have a suitable access-controlled storage area for storage of evidence items.

95. Host forensic tools can be developed in house, be acquired from a licensed vendor or open source. The Head Consultant of the CIR Provider must be able to justify the methodology or techniques and to provide supporting evidence which demonstrates due diligence and real-world experience.

Malware reverse engineering

96. The CIR Provider must be capable of performing malware reverse engineering, both static and dynamic.

97. The CIR Provider must have the capability to reverse engineer any software found on Common Supported Operating Systems.

98. CIR Providers must be able to identify:

    a. capabilities of malware

    b. indicators of Compromise (IOC) to use for detection of activity

    c. relationships between malware samples and other known samples to identify the likely actor behind the attack

99. CIR Providers may be able to fully reverse engineer malware samples to the point of being able to identify flaws in the software or write their own compatible enquiry tools.

100. Incident responders from the CIR Provider will have to handle malware samples and must have sufficient understanding to ensure that they do not accidentally infect any systems.

Ad hoc tooling

101. CIR Providers must have a recorded process for internal and external sign-off on ad hoc tools developed by the incident response team for dealing with specific issues that come up while dealing with an incident. The internal process must involve ensuring that the Head Consultant is aware of any risks of deploying the capability and have accepted them. The external sign-off process must involve the Target Organisation being made aware of any risks of deploying the capability and accepting them.

Commitment to team capability development and R&D

102. As tools, techniques and procedures within cyber incidents are constantly evolving, CIR Providers must demonstrate how they develop both their personnel and their technical capabilities.

103. CIR Providers must demonstrate both training pathways used to train up new staff, and dedication to continuous professional development.

104. CIR Providers must demonstrate regular due diligence reviews of their tools and capabilities as outlined in the sections above to ensure they remain fit for purpose.

Awareness of Operational Technology issues

105. CIR Providers must be aware of threats against Operational Technology (such as PLCs/SCADA) and have a process workflow that can accommodate them.

106. CIR Providers must demonstrate that they would be able to identify and work with subject matter experts (SMEs) in Operational Technology, whether those experts are in-house or externally contracted by the CIR Provider, to assist in resolving a Target Organisation's incident.

10. Reporting and interaction with external stakeholders

107. The CIR Provider may be required to offer assistance or representations to internal and external bodies or have interaction with UK or international entities. These include:

External and internal legal counsel

108. CIR Providers are not expected to offer legal counsel to the Target Organisation.

109. CIR Providers must be aware of how to work with legal counsel without conflicting messaging or advice.

110. CIR Providers must have an awareness of compliance and reporting procedures likely to be relevant to an incident in that sector.

111. Insurance companies may need to be aware of the incident, and they will have their own legal counsel with an interest in the incident response and remediation process.

Regulators

112. The CIR Provider must be able to show evidence of having successfully dealt with incidents in regulated sectors (for example sectors regulated by the Network and Information Systems Regulations 2018).

113. Should the CIR Provider be required to interact with regulators, then a workflow and clear documentation must be presented to the Target Organisation. The Target Organisation is responsible for reporting to regulators. The CIR Provider is not expected to be able to advise a Target Organisation on their regulatory compliance. The role of the CIR Provider is limited to understanding the regulatory context and the implications of that for incident response and remediation, and supporting the Target Organisation by providing the technical input for any regulatory notification the Target Organisation decides to make.

114. The CIR Provider must be capable of preparing the documentation for reporting. Only the Target Organisation is accountable to the regulator, and therefore responsible for complying with the regulatory obligations (including submission of any reports or notifications).

115. The CIR Provider must have experience of dealing with cyber-enabled personal data breaches where the Target Organisation is required to notify the Information Commissioner's Officer under GDPR, and make a data subject notification.

Law enforcement

116. The CIR Provider must be able to show evidence of having successfully worked on incidents that have involved law enforcement.

117. The CIR Provider may be asked to represent the Target Organisation if legal proceedings have occurred at any level. The CIR Provider should ensure that any investigation conducted on the Target Organisation's system is carried out in a way that will enable the evidence to be presented in legal proceedings in any relevant jurisdiction.

118. CIR Providers must be able to show evidence of having successfully worked on incidents where both the NCSC and law enforcement are involved in the investigation, and be able to demonstrate that they understand how the NCSC and law enforcement work together.

Multi-national incidents

119. The CIR Provider must be able to demonstrate experience of successfully dealing with multi-jurisdictional or multi-national organisations incidents. Large Target Organisations (ie those with international presence) may have differing governing or reporting bodies, which may request specific information.

120. The CIR Provider must be able to synchronise a range of actions across the estate, including different time zones and countries (particularly for remediation).

11. Retainer model

121. CIR Providers may be retained by Target Organisations in order to speed up the initial engagement process. In this case, all other details of the processes listed previously must be adhered to and the engagement point will be considered to the point at which the Target Organisation agrees the initial scope of work.

Appendix A: Example scope of work

122. At the outset the scope of work may cover some or all of the below areas.

123. Timescales:

    a. start date
    b. estimated/expected end date
    c. gate or stage expected targets
    d. service level agreements (SLA)
    e. dates/times when stakeholders should expect updates and communication

124. Dependencies and requirements:

    a. technical or infrastructure information/schematics
    b. access to certain areas of the business

125. Bespoke resource and support:

    a. point of contacts for business areas affected
    b. requirements for software/hardware documentation or training
    c. prerequisite information or work required

126. Workload parameters:

    a. defined stage of the incident (preparation, detection & analysis, containment, remediate & eradication or recovery)
    b. specific areas of the business to focus on or avoid
    c. regulation and legal

127. Clear separation of duties:

    a. head consultant to be main point of contact for triage
    b. handovers between the CIR Provider and the Target Organisation
    c. dedicated resource to be allocated to the specific area of the business

128. Expected results:

    a. caveats in finishing the work
    b. desired outcome that the Target Organisation expects and that the CIR Provider can meet
    c. future tasks defined
    d. change in scope may alter the original expected outcome

129. Projected fees:

    a. charge rate (e.g. rate card or blended rate listing)
    b. costs split per investigation/recovery workstream
    c. the CIR Provider must be capable of operating and offering 24/7 support, acknowledging that the Target Organisation may not wish to pay for this level of service
    d. total billable days allotted to the incident may be divided between certain areas of the business and should align to an agreed upon SLA (different operational dependencies)

Appendix B: Evidence required

130. A combination of case studies and personnel profiles must be provided to demonstrate the competencies and delivery capabilities outlined in the standard.

Case studies

131. CIR providers must submit 4 case studies from the last 24 months. Case studies must include the following information:

132. Name of Target Organisation (or relevant Target Organisation set, if case study needs to be anonymised).

133. Nature of initial approach and engagement.

134. Investigative steps undertaken, including any operational constraints arising from Target Organisation setup and actions taken to overcome these limitations.

135. Technical analysis of the malware, attack vector, any exfiltrated data identified and attacker behaviour and the use of this analysis in informing the following:

    a. adversary attribution derived from technical analysis and TI

    b. analysis and understanding of the attacker, their MO and normal target groups

    c. identification of adversary infrastructure used and the use of this information within internal TI development

    d. determining the capability of the attacker (e.g. the technical capability of the attacker

136. Feedback and reporting to Target Organisation (or relevant Target Organisation set).