SFJ CO7
Conduct network investigations

Overview

This standard covers conducting investigations where part or all of the crime is conducted over, or against, networks. It may include, but is not limited to, serious network intrusions which overcome IT systems' architectures and defences.

SFJ CO7
Conduct network investigations

Performance criteria

You must be able to:

P1 assess all **immediately available electronic evidence**, determine its volatility and take all necessary steps to preserve it

P2 assess all other readily available evidence, information and intelligence related to the initial **lines of enquiry**

P3 investigate the **nature**, **cause** and **consequences** of a threat based on the evidence, information and intelligence

P4 conduct a **risk assessment**, assess the **factors** likely to impact on the investigation and take the appropriate action

P5 check that the necessary **authorisations** are in place, if appropriate

P6 determine the geographical and legal jurisdictions that apply and take any necessary steps to preserve and obtain evidence from abroad

P7 identify the need for any **additional support** with the investigation and take the appropriate action

P8 identify victim(s) and potential witnesses in accordance with legislation and policy

P9 take the appropriate steps to identify and deal with any suspect(s)

P10 provide appropriate support for the immediate needs of victims, witnesses and suspects

P11 brief others about the status of the investigation, where appropriate, to ensure continuity

P12 pass on information and intelligence that may be relevant to other actions promptly to the appropriate contact

P13 fully document all decisions, actions, options and rationale related to the **lines of enquiry**, in accordance with current policy and legislation, and create evidential or intelligence product if appropriate

P14 maintain full and accurate records of the examination and investigation for audit log purposes

P15 provide a report on the investigation and provide other briefings as necessary

SFJ CO7
Conduct network investigations

Knowledge and understanding

You need to know and understand:

K1 legal and organisational requirements
- K1.1 current, relevant legislation, policies, procedures, codes of practice, guidelines and applicable standards for conducting network investigations
- K1.2 current, relevant legislation and other organisational requirements
- K1.3 the impact of your actions on victims and witnesses

K2 networks
- K2.1 web site structures and protocols
- K2.2 web applications, coding and vulnerability
- K2.3 fixed line and wireless network and communication protocols
- K2.4 fixed line and wireless network topology and devices
- K2.5 fixed line and wireless network based attack and vulnerability methods
- K2.6 fixed line and wireless network security methods and procedures
- K2.7 fixed line and wireless network interception methods
- K2.8 voiceover internet protocol (VOIP)
- K2.9 digital encryption, public key infrastructure (PKI) and virtual private network (VPN)
- K2.10 how to identify and deal with systems running methods of protecting and concealing electronic information including encryption
- K3.12 the types of operating systems that you may come across and how to deal with these

K3 network investigations
- K3.1 how to obtain evidence, information and intelligence for a network investigation
- K3.2 the sources of relevant evidence, information and intelligence
- K3.3 how to assess the available information and intelligence for a network investigation
- K3.4 how to assess the factors that may impact on the network investigation
- K3.5 the additional support which is available and may be required for the network investigation
- K3.6 how to maximise useful evidence and minimise loss of potential evidence

K4 documentation
- K4.1 the types of documentation that must be completed
- K4.2 the purpose of documenting information on investigations

SFJ CO7
Conduct network investigations

Scope/range related to performance criteria

1 Nature
- 1.1 internal
- 1.2 external
- 1.3 denial of service
- 1.4 directed
- 1.5 random

2 Cause
- 2.1 software vulnerability
- 2.2 privilege escalation
- 2.3 physical security breach
- 2.4 personnel breach
- 2.5 social engineering

3 Consequences
- 3.1 loss or compromise of data
- 3.2 denial of service
- 3.3 theft of goods, services or intellectual property
- 3.4 breach of security or confidentiality
- 3.5 economic loss or gain
- 3.6 public confidence and reputation damage

4 Immediately available electronic evidence
- 4.1 presented volatile evidence
- 4.2 portable and mobile electronic devices
- 4.3 remotely stored
- 4.4 live session/on-screen data
- 4.5 mass data storage devices
- 4.6 communications service providers and registry records

5 Risk assessment
- 5.1 health and safety
- 5.2 physical integrity of the evidence
- 5.3 continuity
- 5.4 legality
- 5.5 authority
- 5.6 priority
- 5.7 commercial and business impact

6 Factors
- 6.1 vulnerability
- 6.2 language
- 6.3 culture
- 6.4 lifestyle
- 6.5 repeat/linked incidents
- 6.6 geographical and legal jurisdiction
- 6.7 technological complexity
- 6.8 social and economic impact

7 Authorisations
- 7.1 preservation
- 7.2 capture

7.3 contract or due diligence
7.4 consent
7.5 limitation

8 Additional support

8.1 specialist support
8.2 line management
8.3 external agencies and consultancies
8.4 software and hardware manufacturers
8.5 computer emergency response teams (CERT)

9 Lines of enquiry

9.1 sources of electronic evidence
9.2 suspects
9.3 witnesses/victims
9.4 forensic/scientific
9.5 intelligence
9.6 property

This standard builds on the skills and knowledge described in SFJ CO6.

SFJ CO7
Conduct network investigations

Links to other NOS

SFJ CO7
Conduct network investigations

Developed by	Skills for Justice
Version number	2
Date approved	January 2012
Indicative review date	December 2016
Validity	Current
Status	Original
Originating organisation	Skills for Justice
Original URN	SFJ CO7
Relevant occupations	Public Services; Public Services and Other Associate Professionals
Suite	Countering Cybercrime
Key words	e-crime, cybercrime, conduct, network, investigation, investigations