## Higher National Unit Specification

## General information

**Unit title:** Securing Network Devices (SCQF level 7)

**Unit code:** J0HE 34

**Superclass:** CC

**Publication date:** June 2018

**Source:** Scottish Qualifications Authority

**Version:** 01

## Unit purpose

The purpose of this unit is to introduce learners to the basic techniques used to protect digital devices that are part of a computer network. This is a **specialist** unit, intended for learners with an interest in computing or computer science; it is particularly suitable for those with a vocational interest in cyber security.

The unit covers the knowledge and skills involved in securing networks to defend against contemporary threats. The knowledge covered includes both internal and external threats along with mitigation techniques. The skills covered include the application of different defence methodologies in a small to medium-sized network, and the impact that increased security can have on end-users.

The unit explores modern security concerns that relate to networked devices, including different threats that exist internally and externally, which include, but are not limited to, poorly secured hardware, software vulnerabilities, misconfiguration, end users, malicious users/software and physical security concerns.

This unit relates to the learners' vocational interests by engaging them in the methodologies that are used to secure modern networks. This allows the learner to grasp the primary concepts required to develop and maintain a network that is secure from various threats, while still maintaining a network that is functional for end users. The ability to create a network that is increasingly secure but still usable will assist the learner in their vocation field of interest.

On completion of this unit, learners will have an understanding of the concepts of modern threats to a network and the different methodologies used to mitigate such threats, and be able to plan, design, and build a network that is secure and functional to support the challenges in the vocational field.

## Higher National Unit Specification: General information (cont)

**Unit title:** Securing Network Devices (SCQF level 7)

## Outcomes

On successful completion of the unit, the learner will be able to:

1 Describe mitigation techniques for threats to a network.
2 Implement different forms of security on end devices or servers.
3 Implement different forms of security on intermediary networking devices.
4 Secure a small to medium-sized network.

## Credit points and level

1 Higher National unit credit at SCQF level 7: (8 SCQF credit points at SCQF level 7)

## Recommended entry to the unit

No previous knowledge or experience is required for the completion of this unit. However, it would be beneficial if learners possessed previous knowledge or skills in general computing and network functionality, or experience in computer science.

## Core Skills

Opportunities to develop aspects of Core Skills are highlighted in the support notes for this unit specification.

There is no automatic certification of Core Skills or Core Skill components in this unit.

## Context for delivery

If this unit is delivered as part of a group award, it is recommended that it should be taught and assessed within the subject area of the group award to which it contributes.

The unit J0HB 34 *Penetration Testing* would be a suitable unit to run in parallel with this unit, as the unit relates to the testing of secure computer network systems.

## Equality and inclusion

This unit specification has been designed to ensure that there are no unnecessary barriers to learning or assessment. The individual needs of learners should be taken into account when planning learning experiences, selecting assessment methods or considering alternative evidence.

Further advice can be found on our website **www.sqa.org.uk/assessmentarrangements**.

## Higher National Unit Specification: Statement of standards

## Unit title: Securing Network Devices (SCQF level 7)

Acceptable performance in this unit will be the satisfactory achievement of the standards set out in this part of the unit specification. All sections of the statement of standards are mandatory and cannot be altered without reference to SQA.

Where evidence for outcomes is assessed on a sample basis, the whole of the content listed in the knowledge and/or skills section must be taught and available for assessment. Learners should not know in advance the items on which they will be assessed and different items should be sampled on each assessment occasion.

## Outcome 1

Describe mitigation techniques for threats to a network.

### Knowledge and/or skills

- Hardware, software and other threats to computer networks including malware
- Types of network security threat (logic and resource)
- Physical security techniques to mitigate environmental or accessibility concerns
- Best practice security techniques for domains/workgroups
- Permissions of users, devices, and/or software on networks
- Access control lists, packet filtering, scanning, and quarantine
- Encryption of static/in motion data
- Network security policies

## Outcome 2

Implement different forms of security on end devices or servers.

### Knowledge and/or skills

- Local security setting implementation
- Domain security policies
- Domain permissions
- Virus protection
- Security of remote access to network devices

## Outcome 3

Implement different forms of security on intermediary networking devices.

### Knowledge and/or skills

- Access security for intermediary networking devices
- Physical security on access level devices
- Security of end device access to a wireless network
- Minimisation of the size of broadcast domains
- Restriction on network traffic between separate IP networks

## Higher National Unit Specification: Statement of standards (cont)

## Unit title: Securing Network Devices (SCQF level 7)

## Outcome 4

Secure a small to medium-sized network.

### Knowledge and/or skills

- Assessment on security of a network using penetration tools and existing documentation
- Security concepts to be used within a network using access control lists
- Testing security concerns where possible
- Securing possible vulnerabilities

### Evidence requirements for this unit

Learners will need to provide evidence to demonstrate the knowledge and/or skills across all outcomes. The evidence requirements for this unit will take two forms.

1 Knowledge evidence
2 Product evidence

The **knowledge evidence** will relate to Outcome 1. Knowledge evidence is required for all knowledge and/or skills statements. The evidence may be produced over an extended period of time in lightly controlled conditions. The amount of evidence may be the **minimum** required to infer competence. For example, learners need only describe the most common hardware and software threats, and demonstrate a basic understanding of social engineering.

The knowledge evidence may be sampled when testing is used. In this case, the evidence must be produced under controlled conditions in terms of location (supervised), timing (limited) and access to reference materials (not permitted). The sampling frame must include the majority of knowledge and skill statements and must always include:

- Hardware and software threats to computer networks including malware
- Physical security techniques to mitigate environmental or accessibility concerns
- Types of network security threat (logic and resource)
- Network security policies

The **product evidence** will relate to Outcomes 2, 3 and 4. It will demonstrate that the learner has gained the practical ability required to secure **at least one** network by building up the level of defence at each part of the network in one larger topology. The learner should apply several security mechanisms to both end devices and intermediary devices. This evidence may be produced over the life of the unit, under loosely controlled conditions. The evidence must be produced by the learner, without assistance.

The evidence for this unit may be written or oral or a combination of these. Evidence may be captured, stored and presented in a range of media (including audio and video) and formats (analogue and digital). Particular consideration should be given to digital formats and the use of multimedia.

## Higher National Unit Specification: Statement of standards (cont)

**Unit title:** Securing Network Devices (SCQF level 7)

The SCQF level of this unit (level 7) provides additional context on the nature of the required evidence and the associated standards. Appropriate level descriptors should be used when making judgements about the evidence.

When evidence is produced in loosely controlled conditions it must be authenticated. The Guide to Assessment provides further advice on methods of authentication.

The support notes section of this specification provides specific examples of instruments of assessment that will generate the required evidence.

## Higher National Unit Support Notes

## Unit title: Securing Network Devices (SCQF level 7)

Unit support notes are offered as guidance and are not mandatory.

While the exact time allocated to this unit is at the discretion of the centre, the notional design length is 40 hours.

## Guidance on the content and context for this unit

This unit is intended for those with an interest in the overall security of network devices, who wish to gain a deeper understanding of how different networks can be secured against threats, both external and internal. The unit is for those that aim to understand what threats exist and how to defend or mitigate them on multiple levels of the network, from end devices to core network devices. The unit is particularly suited to those with some computer networking background.

The aim of the unit is to show learners that, regardless of the network topology and overall set-up, mechanisms can be put in place at every level to protect data or the network itself. The unit has four outcomes covering a range of theory and practice. Although all of the outcomes will provide a theoretical aspect, Outcome 1 is predominately theoretical and Outcomes 2, 3, and 4 will have a larger practical element.

The unit should encourage the learner to consider the scale of the network and where security mechanisms could be applied for the greatest effect. This should allow the learner to progress to a more adaptive methodology rather than a rigid one. In turn, this should provide the learner with a technical skill set that can be taken and applied in industry.

The unit would serve as an excellent introduction to network security and could result in the learner wishing to progress their understanding of network security. Below is a list of vendor certifications that they may wish to progress to over time:

- Microsoft MTA ‘Security Fundamentals’
- Microsoft MTA ‘Network Fundamentals’
- Cisco CCT
- Cisco CCENT
- Cisco CCNA Routing and Switching
- Cisco CCNA Security

This course (in addition to the above certifications) would provide the learner with the knowledge required to begin a career in technical support for users, network administration, network security consultancy, and many others.

Please note that the following guidance, relating to specific outcomes, does not seek to explain each knowledge/skills statement, which is left to the professionalism of the teacher. It seeks to clarify the statement of standards where it is potentially ambiguous. It also focuses on non-apparent teaching and learning issues that may be over-looked, or not emphasised, during unit delivery. As such, it is not representative of the relative importance of each knowledge/skill.

## Higher National Unit Support Notes (cont)

## Unit title: Securing Network Devices (SCQF level 7)

### Outcome 1

This outcome relates to the threats that currently exist. Although each knowledge/skills statement has a focus area, the overall outcome should encourage the learner to be adaptive to any threat that is presented.

Learners should know why the security of a network is important and that the threats are ever-changing based on current trends. The learners should understand what mitigation techniques should be used and when/where to apply them: from securing core devices in an air-conditioned room with restricted access, to the updating of anti-virus software on an end device. They should understand the concept that there is no 'one size fits all' when it comes to the security of a network, and that different threats will require different mitigation techniques.

In addition, the learner should begin to understand how constant maintenance is required to maintain a secure network, and some basic security principals or best practices should be applied, such as locking the network down, and slowly providing access, as and when needed.

### Outcome 2

This outcome focusses on the security of end devices, such as PC and servers. The main focus of this area should be the overall security of an end device, not just something as simple as accessibility to files.

The learner should understand the purpose of the different in-built mechanisms, such as firewalls and anti-virus software. As well as administrator applied policies, such as group policy, mandatory access controls or local/domain password policies.

The focus should be practical in nature, providing both the method of configuration and the impact this will have on the system (where possible). This could include restricting a user's ability to install programs without administrator approval, to separating end devices and servers on to separate VLANs, stopping users from being able to access key domain systems. It is possible to utilise a virtual environment for the practical element of this outcome and/or a practical lab build environment.

### Outcome 3

This outcome focusses on the security of intermediary devices in a network, such as routers, switches or firewalls.

This outcome can focus on the security of the device itself and on the methods which can be used to secure traffic on the network. From securing access to a router over SSH, to using switchport security, to shutdown ports when an unrecognised MAC address is detected, or a Wi-Fi equivalent.

The focus should be practical in nature, providing both the methods of configuration and the impact this could have on the system and/or network. It is possible to utilise a virtual environment for the practical element of this outcome and/or a practical lab build environment.

## Higher National Unit Support Notes (cont)

## Unit title: Securing Network Devices (SCQF level 7)

**Outcome 4**

This outcome focusses on the assessment and application of appropriate mitigation techniques against network threats in small to medium-sized networks, such as Small Office Home Office (SOHO) networks or branch networks.

The aim of this outcome is to apply concepts learned in Outcomes 1, 2 and 3 in a practical environment.

## Guidance on approaches to delivery of this unit

Although this unit provides a large body of knowledge, it is recommended that it be delivered in a practical manner in order to provide the learner with experience of implementation and to encourage adaptive approaches to different possible solutions.

This unit could be delivered alongside J0HB 34 *Penetration Testing*, as the goal of penetration testing is to find security flaws within secure networks. This would again encourage the learner to re-assess and adapt to issues presented. In addition, this should give the learner experience in testing their own applied security mechanisms.

The large quantity of practical work will likely require access to physical/specialist resources. This could include, but is not limited to:

- GUI or CLI based end devices/server .ISO
- Oracle virtual box
- Cisco packet tracer or GNS3
- Managed routers/switches

The order of the unit is open to interpretation but it is recommended that the outcomes be delivered sequentially. However, it is possible to deliver Outcomes 2, 3 and 4 while constantly providing content from Outcome 1 that relates to the practical activities at hand. For example, learners could build an end device and server, and apply different security mechanisms to them, while learning why the mechanism is being applied and what it aims to prevent.

In addition to this delivery method, some suggested activities could entail having a member of internal IT staff briefly detail security concepts used with the facility, or speaking to local data centres to provide a tour of their facility to demonstrate physical security mechanisms in place.

A suggested distribution of time, across the outcomes, is:

Outcome 1: 10 hours
Outcome 2: 10 hours
Outcome 3: 10 hours
Outcome 4: 10 hours

Summative assessment may be carried out at any time. However, when testing is used (see evidence requirements), it is recommended that this be carried out towards the end of the unit (but with sufficient time for remediation and re-assessment). When continuous assessment is used (such as the use of a web log), this could commence early in the life of the unit and be carried out throughout the duration of the unit.

There are opportunities to carry out formative assessment at various stages in the unit. For example, formative assessment could be carried out on the completion of each outcome to ensure that learners have grasped the knowledge contained within it. This would provide assessors with an opportunity to diagnose misconceptions, and intervene to remedy them before progressing to the next outcome.

## Guidance on approaches to assessment of this unit

Evidence can be generated using different types of assessment. The following are suggestions only. There may be other methods that would be more suitable to learners.

Centres are reminded that prior verification of centre-devised assessments would help to ensure that the national standard is being met. Where learners experience a range of assessment methods, this helps them to develop different skills that should be transferable to work or further and higher education.

Assessment for this unit can be achieved in a number of ways.

Knowledge assessments and evidence can be generated in the following summative formats:

1 A selected response test consisting of four options (one key) with a pass mark of 60%. There may need to be scenario-type questions to assess the learner's competency. The test could consist of a relatively high number of questions (30 or 40 for example), lasting an hour, covering Outcome 1 and sampling all of the knowledge statements where possible.

2 An extended response scenario could be provided requiring that the learner research and investigate a feasible solution within the environment, to a proposed series of problems. The solution could be documented in multiple formats, such as written, oral, or recorded response. This could consist of ten problems, all requiring possible solutions. In order to achieve a pass mark of 60%, the learner would have to develop a solution for six or more problems and document them appropriately. This could be done over the course of 1 hour and 30 minutes, covering Outcome 1 and sampling all of the knowledge statements where possible.

The primary focus should be on the content of Outcome 1 and learners should be able to demonstrate an understanding of the different threats and what can be done to mitigate the threat at hand.

## Higher National Unit Support Notes (cont)

## Unit title: Securing Network Devices (SCQF level 7)

The practical element could be assessed by the following formative formats:

1 Demonstration of a small network with security mechanisms / mitigation techniques in use. This could be an open-book approach, where the learner is permitted the use of external resources to research different mitigation techniques that could be applied to a predesigned network. This assessment should be recorded by appropriate means, to provide evidence. The overall understanding and justification of choices is key, but the learner will have to demonstrate understanding from Outcomes 2, 3 and 4. A prominent security mechanism from each outcome would be sufficient to gain a pass.

2 Demonstration of each outcome could be assessed independently per outcome. This could be an open-book approach, where the learner is permitted the use of external resources to research different mitigation techniques to secure end devices. Then, as part of another assessment, apply security to intermediary devices, such as switches; and finally, overall network security, such as firewall access control lists. When all concepts are built together this should create an overall secure network. The overall understanding and justification of choices is key, but the learner will have to demonstrate understanding from Outcomes 2, 3 and 4. A prominent security mechanism from each outcome would be sufficient to gain a pass.

A more contemporary approach to assessment would involve the use of a web log (blog) to record learning (and the associated activities) throughout the life of the unit. The blog would provide knowledge evidence (in the descriptions and explanations) and product evidence (using, for example, video recordings) but in addition a learner demonstrating their discovery of solutions. The blog should be assessed using defined criteria to permit a correct judgement about the quality of the digital evidence. In this scenario, every knowledge and skill must be evidenced; sampling would not be appropriate.

Formative assessment could be used to assess learners' knowledge at various stages throughout the life of the unit. An ideal time to gauge their knowledge would be at the end of each outcome. This assessment could be delivered through an item bank of selected response questions, providing diagnostic feedback to learners (when appropriate).

If a blog is used for summative assessment, it would also facilitate formative assessment since learning (including misconceptions) would be apparent from the blog, and intervention could take place to correct misunderstandings on an on-going basis.

## Opportunities for e-assessment

E-assessment may be appropriate for some assessments in this unit. By e-assessment we mean assessment which is supported by Information and Communication Technology (ICT), such as e-testing or the use of e-portfolios or social software. Centres which wish to use e-assessment must ensure that the national standard is applied to all learner evidence and that conditions of assessment as specified in the evidence requirements are met, regardless of the mode of gathering evidence. The most up-to-date guidance on the use of e-assessment to support SQA's qualifications is available at **www.sqa.org.uk/e-assessment**.

## Higher National Unit Support Notes (cont)

## Unit title: Securing Network Devices (SCQF level 7)

## Opportunities for developing Core and other essential skills

This unit allows for opportunities to develop the following Core Skills:

- *Communication*
- *Information and Communication Technology*
- *Problem Solving*
- *Working with others*

Written communication can be utilised throughout Outcomes 1, 2, 3 and 4, through the use of review and research within all aspects of the unit.

Learners should be encouraged to access and create content, such as topologies and videos demonstrating work performed; this, in turn, can be applied to a blog. Such a Core Skill would be developed within Outcomes 2, 3 and 4 of this unit.

Problem solving should be a concept that is developed throughout the entire unit, as it should encourage the adaptive thinking required to overcome the ever-changing environment.

Although working with others is not directly required, team working can be encouraged and used throughout practical activities of the unit in Outcomes 2, 3 and 4.

## History of changes to unit

| Version | Description of change | Date |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## General information for learners

## Unit title: Securing Network Devices (SCQF level 7)

This section will help you decide whether this is the unit for you by explaining what the unit is about, what you should know or be able to do before you start, what you will need to do during the unit and opportunities for further learning and employment.

This is an introductory unit into the concepts and practice of network security, for those with existing networking knowledge. It is suitable for learners who are undertaking a wide range of qualifications.

The unit covers the theory and practice of network security. Learners would benefit from this undertaking this unit if they have interest in overall security of networks from internal and external threats.

The unit covers the following topics:

- The importance of network security in modern society
- Application of physical security techniques for all network devices
- Best practice security techniques for domains/workgroups
- What different types network threats that exist
- What different mitigation techniques are available
- How to implement different mitigation techniques
- How to develop a customised security plan for different networks
- The different tools available for network security

Each topic should be covered in broad detail, combining both practical and theoretical elements together. It will be delivered in an accessible and interesting way, which may include the use of audio and video to enliven learning.

Several concepts within the unit are theoretical but should be married up to practical activities. These will apply to possible future job prospects, providing you with hands-on experience and use of tools that would be used in real life environments, such as access control configuration and network permissions within a domain.

Teaching methods will likely include self-learning, researching and group discussion.

This unit can be assessed in a number of ways including, for example, recording of a physical activity or multiple-choice assessment. Regardless of the methods used for assessment, most time will be spent learning, not being assessed.

By the end of this unit you will have developed understanding of how to secure small to medium-size networks, the threats to modern networks and how to continually develop your knowledge of this area of computing. These concepts and techniques can be used in your job and, personally, to continually improve any network's security.

You could progress in to other areas such as Computer Networking, Technical Support, and potentially Ethical Hacking.