Higher National Unit Specification

General information

Unit title: Cyber Resilience (SCQF Level 7)

Unit code: HT9V 34

Superclass:	CB
Publication date:	November 2017
Source:	Scottish Qualifications Authority
Version:	02

Unit purpose

The purpose of this unit is to introduce learners to the essential knowledge, skills and behaviours required to maintain their own cyber hygiene and contribute to workplace cyber resilience. It also introduces key knowledge of, and skills in, cyber security.

This unit is a non-specialist unit, suitable for a wide range of learners undertaking a variety of qualifications. No prior knowledge or experience of cyber security or computer science is required.

The unit covers a wide range of knowledge, skills and behaviours. The knowledge covered includes knowledge of the most common threats to data security; knowledge of the steps that can be taken to reduce the risks posed by these threats; and knowledge of what to do if security is compromised. The skills covered include skills in securing digital devices; skills in maintaining digital devices; and skills in data recovery. The behaviours include acting responsibly and safely when using digital devices; avoiding social engineering attacks; and responding appropriately when an attack takes place. The unit also explores the tension between security and privacy.

On completion of this unit, learners will know the main threats to data security, know how to minimise the risk from these threats, and know how to respond if an attack takes place.

Outcomes

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

1 Maintain cyber hygiene.
2 Contribute to cyber security in a working environment.
3 Respond appropriately to a cyber attack.

Higher National Unit Specification: General information (cont)

Unit title: Cyber Resilience (SCQF Level 7)

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

This is an introductory unit in the field of cyber security and, as such, there are no prior knowledge or skills required before undertaking this unit. However, it would be beneficial if learners possessed digital skills, which could be evidenced by possession of the Core Skill in *Information and Communication Technology* at SCQF level 5 or completion of the national progression awards in Cyber Security at SCQF levels 4, 5 or 6.

Core Skills

Achievement of this Unit gives automatic certification of the following:

Complete Core Skill	Problem Solving at SCQF level 5
Core Skill component	None

Opportunities to develop aspects of Core Skills are highlighted in the Support Notes for this Unit specification.

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.

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: Cyber Resilience (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

Maintain cyber hygiene.

Knowledge and/or skills

- Definition of cyber hygiene, cyber security and cyber resilience
- Cyber security threats to individuals
- Common vulnerabilities in digital devices
- Unsafe online behaviours
- Social engineering techniques
- Cyber security tools and techniques for individuals including encryption
- Methods of authentication including strong passwords
- Data security and personal privacy
- Skills in configuring and securing digital devices

Outcome 2

Contribute to cyber security in a working environment.

Knowledge and/or skills

- Cyber security threats to groups and organisations
- Common vulnerabilities in digital networks
- Cloud computing and data security
- Cyber security tools and techniques for groups and organisations
- Corporate cyber security policies
- Unsafe network activities
- Physical security of data
- Skills in maintaining network security

Outcome 3

Respond appropriately to a cyber attack.

Higher National Unit Specification: Statement of standards (cont)

Unit title: Cyber Resilience (SCQF Level 7)

Knowledge and/or skills

- Types of cyber attack
- Consequences of each type of cyber attack
- Responses to cyber attacks
- Backup and recovery methods and techniques
- Disaster recovery
- Business continuity

Evidence requirements for this unit

Learners will need to provide evidence to demonstrate their knowledge and/or skills across all outcomes by showing that they can produce:

1 knowledge evidence (Outcomes 1, 2 and 3)
2 product evidence (for Outcomes 1, 2 and 3)
3 performance evidence (for Outcomes 1, 2 and 3)

The knowledge evidence will comprise the underpinning knowledge required in Outcomes 1, 2 and 3. Evidence is normally required for all knowledge and/or skills statements except those explicitly relating to skills. However, sampling is permissible in certain circumstances (see below). The level of treatment for each topic need not be deep; the focus of the evidence is breadth, not depth.

The knowledge evidence may be sampled when testing is used. Given that the focus is breadth rather than depth, sampling must be wide and shallow (such as the use of selected response or short answer questions) rather than narrow and deep (such as the use of an extended response question on one element of the knowledge domain). When testing is used, it must be under supervised conditions and it must be controlled in terms of location, timing and access to reference materials.

The product evidence will demonstrate that the learner has configured and secured at least one digital device (Outcome 1), maintained network security over an extended period (Outcome 2), and responded to at least two cyber attacks (Outcome 3). The cyber attacks may be real or simulated attacks. The evidence may take any appropriate form including narrative descriptions of configurations and settings (for Outcome 1), descriptions of user actions to maintain network security, and descriptions of user actions in response to cyber attacks (Outcome 3). Alternative (or additional) forms of evidence include configuration logs and witness testimony. The evidence may be produced in an actual or simulated workplace. This evidence may be produced over the life of the unit, under loosely controlled conditions (including access to reference materials). Authentication will be necessary (see below).

The performance evidence will demonstrate correct behaviours when learners use digital devices and networks as required in Outcomes 1, 2 and 3. The correct behaviours will be pre-defined, and learners must be observed using digital devices and digital networks so that they can be judged against these behavioural standards. When appropriate, it is permissible to assess learners by exception, whereby they are presumed to adhere to the defined standards unless their conduct demonstrates otherwise.

Unit title: Cyber Resilience (SCQF Level 7)

The SCQF level of this unit provides additional context on the nature of the required evidence and the associated standards. The following level descriptors are particularly relevant to the evidence.

- An overall appreciation of the body of knowledge.
- Knowledge that is embedded in the main theories, concepts and principles.
- Apply knowledge and skills in practical contexts.
- Use some of the basic and routine professional skills, techniques, practices and materials.
- Use a range of approaches to address defined and/or routine problems.
- Exercise some initiative and independence in carrying out defined activities at a professional level.
- Take account of own and others' roles and responsibilities when carrying out tasks.

These level descriptors should be used (explicitly or implicitly) when making judgements about the evidence.

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

The *Guidelines on Approaches to Assessment* (see the support notes section of this specification) provides specific examples of instruments of assessment.

Higher National Unit support notes

Unit title: Cyber Resilience (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

The content of this unit provides a basic introduction to the principles and practice of cyber resilience. Cyber Resilience refers to an entity's ability to continuously deliver the intended outcome despite adverse cyber events. The focus of the unit is to make the learner aware of how their skills and behaviours can affect their digital security and how this affects organisational resilience. The unit is intended for non-specialists and may be offered as part of a wide range of programmes and the level of treatment of each topic should reflect this. For example, the learner will not be responsible for dealing with a cyber attack within an organisation, but know what part they have to play in the response to an attack.

Outcome 1 covers a person’s cyber hygiene, what this means and what they can do to improve it. Whether at work in the public or private sector, or on personal computers and devices, there is a greater need than ever to be vigilant. In order to accomplish this, good cyber hygiene must be practised daily. This outcome should cover the theory behind cyber security with an emphasis on cyber hygiene, including:

- The definitions of cyber hygiene, cyber security and security threats in the current climate and an outline of what steps can be taken to minimise these.
- The threats posed to individuals, this could be risk to personal privacy, bank account compromises, etc.
- The common vulnerabilities in digital devices whether these be computers, laptops, smartphones, 'internet of things' devices such as printers, webcams, thermostats, etc. This should look at how these vulnerabilities can be prevented, such as ensuring software updates are always kept up to date, not opening unknown attachments or links from e-mails.
- Unsafe online behaviours such as clicking on un-verified links, using open wireless networks and using caution on social networking sites.
- What social engineering is and what techniques are commonly applied by social engineers and how this can lead to a breach in security.
- How to use cyber security tools and techniques including the purpose of encryption and how encryption can improve data security.
- The importance of strong passwords and of keeping passwords secure; this should be balanced with the importance of not having to secure a password strategy that results in passwords being written down.
- Outline how data security can impinge on personal privacy. Learners should be made aware of data breach examples and where the data that was stolen ended up and what potentially was used for.

- Skills in configuring and securing digital devices; the importance of anti-virus software in keeping secure and the importance of ensuring it is updated regularly with scheduled updates; also the importance of changing default passwords on devices such as network routers, 'internet of things' devices, this should include default pin number for bluetooth devices.

Outcome 2 builds on Outcome 1 and covers the contribution to cyber security an individual can make in a working environment. This looks at the social/business environment where businesses/organisations' cyber security strategy will have an impact on how individuals behave in a working environment and how individuals can contribute to cyber resilience. This should include:

- The threats posed to groups and organisations, this could be risk to company data, loss of reputation, failure to adhere to current legislation, etc.
- The common vulnerabilities in digital networks, and how these differ from digital devices in the home. This could link to how viruses spread in an organisation and how social engineering is a common way to attack a digital network. Awareness and identification of social engineering threats and how to respond to them. Social engineering is one of the most common ways that hackers can penetrate the security of a system, so having this awareness can greatly reduce this type of threat. The learner should be aware of the forms that social engineering may take and how to respond appropriately.
- The security implications of cloud computing relate to the increased exposure of personal, corporate and government data resulting from this form of shared data storage and access.
- Cyber security tools and techniques that should be carried out regularly in order to contribute to a corporate cyber security strategy. This should build on the cyber hygiene techniques learned in Outcome 1 and relate them to a working environment.
- An awareness of corporate cyber security policies, what is likely to be contained within them and how best to adhere to them given the knowledge gained in Outcome 1.
- Unsafe network activities relate to the behaviours that individuals can engage in that may compromise network security. Examples include: sharing passwords with co-workers, installing unauthorised software, failing to encrypt sensitive communications and disabling security software.
- The importance of physical security of data should be emphasised.
- Skills in maintaining network security relate to the routine (user) activities involved in maintaining network security such as ensuring the security software is active and kept up to date, selecting strong passwords (and regularly changing them), and adhering to network security requirements.

Outcome 3 looks at common cyber attacks and how to respond appropriately to them, which could include (but not limited to):

- Recognising a cyber attack should look at firstly defining what a cyber attack is. It has been defined by the UK's National Cyber Security Centre as 'a breach of a system's security policy in order to affect its integrity or availability. The unauthorised access or attempted access to a system.' Recognising the symptoms of a cyber attack should include (but not be limited to):

- — fake anti-virus messages
- — unwanted browser toolbars
- — redirected internet searches
- — frequent random pop-ups
- — fake e-mails or messages originating from an account
- — online passwords changed
- — unexpected software installations
- — unexplained mouse movements
- — anti-virus or anti-malware disabled and cannot be re-started
- — unexplained money missing from bank accounts

- ♦ The consequences of each type of attack should be explained. For example, a ransomware attack and a denial of service attack have different consequences for individuals, corporations and governments.
- ♦ Appropriate responses to a cyber attack from a corporate and personal viewpoint. These will differ greatly, but both are important to know. In an organisation, the approach to cyber resilience may follow the following five steps: prepare, protect, detect, improve and recover. There should be policies and procedures in place that would be followed in the event of a cyber attack; these procedures would inform all levels in the organisation of what their responsibilities are.
- ♦ An organisation should ensure that the frontline employees are able to recognise threats and report them or report breaches as soon as they are recognised, the emphasis is on preventative maintenance. Employees can be the strong link in defence. The importance of reporting cyber security incidents in an organisation or in a personal context forwarding suspicious e-mails, etc to vendors should be evident.
- ♦ The appropriate action taken will depend on the attack and whether this is a home user, small office/home office or a corporate environment. However, the outcome will get the learner to carry out the tasks required to respond appropriately to a cyber attack which, in general, may include the following steps:
  - — Change password
  - — Backup and important data before that data is lost
  - — Report the incident
  - — Conform to data protection law where appropriate
  - — Disconnect from network

  The learner should document all stages of response and know the importance of doing so. The learner should also review their actions in order to evaluate whether the response was appropriate and effective, and what changes they would look to implement to prevent a similar attack from occurring. They should also review the response taken if a similar attack were to happen again.
- ♦ The learner is made aware of what is meant by disaster recovery and how a business requires policies procedures to enable the recovery or continuation of vital technology infrastructure and systems following a cyber attack (as well as natural or human-induced disasters). Disaster recovery is part of business continuity and should be invoked after a cyber attack to ensure all critical business functions are operational. The importance of backup in disaster recovery should be stressed.
- ♦ Planning a response approach to a cyber security attack. When a breach is discovered, it is essential to act comprehensively and quickly, or it may expose the business to greater liability or the individual to lose personal information or data. When planning the response, it is important that the plan can be put in place quickly, however this needs to be focussed and having plans in place will help to inform the response. The learner should be made aware of standard techniques for responding to attacks.

Unit title: Cyber Resilience (SCQF Level 7)

The unit should be delivered in an appropriate context for the learners and reflect their vocational and personal interests. For example, learners with an interest and/or background in business should be taught in that context. However, all learners must be exposed to a variety of situations and not just those directly relevant to their vocational interests.

Throughout this unit it is vital to present the applications and implications of cyber resilience in a balanced way, neither overstating the opportunities nor understating the threats posed.

Guidance on approaches to delivery of this unit

This unit is intended to be delivered to non-specialists and the approach taken to deliver the unit should take this into account, it is about what a person can do to help protect their own cyber hygiene in the context of helping to improve cyber resilience.

The outcomes may be delivered in the order in which they are written. They have been written with a learning sequence in mind.

The actual distribution of time between outcomes is at the discretion of the centre. However, one possible approach is to distribute the available time as follows:

Outcome 1:	14 hours
Outcome 2:	16 hours
Outcome 3:	10 hours

It is anticipated that the required concepts will be introduced by the teacher and reinforced by appropriate examples.

There is significant scope in this unit to illustrate concepts and skills with case studies of actual or potential cyber breaches to demonstrate the implications of poor cyber hygiene. While the majority of time in this unit will be spent on the theoretical aspects of the unit, these can be explained through real-world examples.

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.

A traditional approach to assessment could satisfy the evidence requirements by using a test and a practical assignment.

Knowledge evidence could be produced using an end of unit test. This test would sample from the knowledge and understanding contained in Outcomes 1, 2 and 3. The test could comprise a number of short answer questions and would be marked and assessed traditionally. For example, the test may comprise of 10 questions, requiring a response comprising no more than one or two paragraphs, selected across all three outcomes, each worth five marks, with the learner responses marked out of 50 and a pass mark of 25. If this approach is taken, it is recommended that some (or all) of the questions combine the knowledge and understanding within and across outcomes. This test would be taken, sight-unseen, in controlled and timed conditions without reference to teaching materials. A suitable duration could be 60 minutes.

Product and performance evidence could be produced using a practical assignment, which would require learners to protect digital devices, maintain network security in routine and non-routine conditions (when the network is under attack) and respond appropriately to cyber attacks. The product evidence could consist of a completed *pro forma*. The performance evidence could consist of a completed observation checklist, which would record learner behaviour (including their responses to cyber attacks) throughout the life of the unit.

A more contemporary approach to assessment could satisfy the evidence requirements by using a web log (blog). This blog would provide knowledge and product evidence by describing the knowledge and skills acquired during the unit. The knowledge evidence would be apparent from the various posts describing and explaining what has been learned; the product evidence could be manifest in the descriptions, images and videos used to record practical activities. A separate observation checklist could be used to provide performance evidence. In this scenario, sampling would not be appropriate; all of the knowledge and skills would have to be evidenced by the blog.

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.

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**.

Opportunities for developing Core and other essential skills

This Unit has the Core Skill of Problem Solving embedded in it. This means that when learners achieve the Unit, their Core Skills profile will also be updated to show they have achieved Problem Solving at SCQF level 5

This unit also provides opportunities to develop some components of the following Core Skill:

- *Information and Communication Technology (ICT)* (SCQF level 6)

Several components of the Core Skill in *Information and Communication Technology (ICT)* may be addressed in this unit. There are opportunities to start software, enter and edit data, locate and extract information, apply a complex search strategy and evaluate information.

History of changes to unit

Version	Description of change	Date
02	Core Skill of Problem Solving at SCQF level 5 embedded.	24/11/2017

Additional copies of this unit specification can be purchased from the Scottish Qualifications Authority. Please contact the Business Development and Customer Support team, telephone 0303 333 0330.

General information for learners

Unit title: Cyber Resilience (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.

The purpose of this unit is to introduce you to the essential knowledge, skills and behaviours required to maintain your own cyber hygiene and contribute to workplace cyber resilience. It also introduces key knowledge of, and skills in, cyber security.

Someone is defined as having good cyber hygiene if they can select and maintain high quality passwords; install and maintain security software on their digital devices; keep their virus definitions up-to-date; run regular security scans on their digital devices; adhere to cyber security policies; protect their personal data; and avoid potential sources of infection. A person with low cyber hygiene may fail to observe one or more of these behaviours, such as not routinely updating their virus definitions or using online services that are known sources of malware.

This unit is a non-specialist unit, suitable for a wide range of learners undertaking a variety of qualifications. No prior knowledge or experience of cyber security or computer science is required.

The unit covers a wide range of knowledge, skills and behaviours. The knowledge covered includes: knowledge of the most common threats to data security; knowledge of the steps that can be taken to reduce the risks posed by these threats; and knowledge of what to do if security is compromised. The skills covered include: skills in configuring digital devices to protect them; skills in maintaining digital devices; and skills in data recovery. The behaviours include: acting responsibly and safely when using digital devices; avoiding social engineering attacks; and responding appropriately if a device is attacked.

The unit also explores the tension between data security and personal privacy.

You may be required to undertake an end of unit test for the knowledge and understanding across all outcomes and a practical task showing how you would configure and secure digital devices, maintain network security and respond appropriately to cyber attacks.

This Unit has the Core Skill of Problem Solving embedded in it, so when you achieve this Unit your Core Skills profile will be updated to show that you have achieved Problem Solving at SCQF level 5.

The unit will provide an opportunity to develop your *Information and Communication Technology (ICT)* Core Skills.