Pearson
BTEC Higher National qualifications in Computing

Pearson-set Theme Release
1st September 2025 to 31st August 2026

Unit 16: Computing Research Project

First Teaching from September 2022

First Certification from September 2023

For use with the following qualifications:

Pearson BTEC Level 5
Higher National Diploma in Computing

Pearson BTEC Level 5
Higher National Diploma in Computing for England

(Also for use with Unit 13 – Computing Research Project in HND in Computing, First Teaching Sep 2018)

Edexcel, BTEC and LCCI qualifications

Edexcel, BTEC and LCCI qualifications are awarded by Pearson, the UK's largest awarding body offering academic and vocational qualifications that are globally recognised and benchmarked. For further information, please visit our qualifications website at qualifications.pearson.com. Alternatively, you can get in touch with us using the details on our contact us page at qualifications.pearson.com/contactus

About Pearson

Pearson is the world's leading learning company, with 35,000 employees in more than 70 countries working to help people of all ages to make measurable progress in their lives through learning. We put the learner at the centre of everything we do, because wherever learning flourishes, so do people. Find out more about how we can help you and your learners at qualifications.pearson.com

References to third party material made in this document are made in good faith. Pearson does not endorse, approve or accept responsibility for the content of materials, which may be subject to change, or any opinions expressed therein. (Material may include textbooks, journals, magazines and other publications and websites.)

All information in this document is correct at time of publication.

Contents

1 Introduction to theme

The Pearson-set theme for use with Unit 16: Computing Research Project is:

Cyber Security

Cybersecurity is the field of computing concerned with the practices, processes, and technologies designed to protect systems, networks, and data from cyberattacks. As our reliance on digital systems has evolved, cybersecurity has become critical in safeguarding sensitive information and allowing organisations and governments to function. The increasing reliance on the reliability and stability of interconnected systems means that the need to combat threats like hacking, data breaches, and malware has intensified.

In 2023 alone, the World Economic Forum estimated that there were about 2,200 cyberattacks every day across the globe. For organisations, an effective cybersecurity strategy ensures business continuity, protects intellectual property, and builds customer trust. For individuals, it safeguards sensitive information and promotes safer online interactions. In society, cybersecurity underpins the digital economy, supports innovation, and reinforces national security. As technologies like cloud computing and IoT become more commonplace, cybersecurity serves as the foundation for a safe, digital future.

Cybersecurity encompasses a wide range of fields, including network technologies and architecture, cloud computing, and encryption algorithms. It involves the deployment of technologies such as intrusion detection systems, and multi-factor authentication, alongside strategies including ethical hacking and threat intelligence. The field of cybersecurity also includes the legal and ethical implications and explores emerging risks associated with technologies such as artificial intelligence and quantum computing.

However, the field also faces significant challenges. Cybersecurity solutions often come with high financial and environmental costs, posing barriers for small businesses and underserved communities. Rapid technological advancements create gaps in expertise, leading to a global skills shortage. Ethical dilemmas, such as balancing privacy with security and addressing biases in AI-driven solutions, further complicate the landscape.

The theme will enable students to explore some of the topics concerned with cybersecurity from the standpoint of a prospective network administrator or cybersecurity specialist. It will provide the opportunity for students to investigate the applications, benefits and limitations of cybersecurity while exploring the responsibilities and solutions to the problems it is being used to solve.

2 Choosing a research objective/question

Students are to choose their own research topic for this unit. Strong research projects are those with clear, well focused and defined objectives. A central skill in selecting a research objective is the ability to select a suitable and focused research objective. One of the best ways to do this is to put it in the form of a question. Students should be encouraged by tutors to discuss a variety of topics related to the theme to generate ideas for a good research objective.

The range of topics discussed, could cover the following areas:

- Insider threats and the risks from employees or partners
- Cybercrime evolution and the trends in cyberattacks and criminal tactics
- Risks to the supply chain from third-party software and vendors
- Mobile security - protecting data on smartphones and tablets
- Deepfake technology and the rise in threats from manipulated media
- Securing critical infrastructure systems from cyberattacks
- Zero trust models and how limiting access can strengthen cybersecurity
- Dark web activities – monitoring and mitigating illegal online markets
- Quantum computing and its implications for cybersecurity
- Cybersecurity and virtualised networks
- Evolution of legislation to deal with current and future cyber threats

The research objective should allow students to broaden their understanding and widen their perspective of being able to explore, argue, prove, and/or disprove a particular objective. The research objective should be feasible, novel, ethical, relevant and ultimately of interest to the student. Guidance for tutors is available in the ***Pearson-set Assignment Guidance document for Unit 16: Computing Research Project*** and templates are provided for both the research proposal and ethics form.

For those centres who have multiple start dates throughout the academic year, for example students beginning their studies on the Higher National Diploma between January and July, the same theme for both Level 4 and Level 5 Pearson-set units may apply (depending on delivery schedules and when students commence the Pearson-set units). If students are in a position of completing the same theme for both Level 4 and 5, centres must ensure that the theme for the Level 5 is addressed in a different context from the topic selected and applied at Level 4.

Please note that if reasonable adjustments are necessary to meet a specific individual student need you are able to adjust internal assessments to take this into account.

Any adjustments must be considered in relation to the centre's policies on equality & diversity and student support.

Further details on how to make adjustments for students with protected characteristics are given in the document *'Pearson Supplementary Guidance for Reasonable Adjustment and Special Consideration in Vocational Internally Assessed Units'* available on our website (http://qualifications.pearson.com).

3 Project evidence / outcomes

It is important to recognise that project work is reliant on gathering information/data that can be analysed. The scale of the project means that there must be time for both primary and secondary research. An advised model would be to use secondary research to provide a context for the students to conduct and interpret primary data collection. The project could then yield data that could be compared with the findings of secondary research information.

In assessing the project, the assessor should be able to see a rationale for the project title, an identification of controversial aspects of the title and of the relevant literature/data sources. This will be based primarily on the student's research proposal. Student research should outline the literature/theories that supports the identified research objective/s and include critical evaluation of central arguments paying attention to whether or not the arguments are logically valid. Throughout their research students should be aware of the importance of clear and consistent use of language and the use of a consistent reference system. Engagement in reflective study of the research process should be evident, with students explaining how their ideas have developed, the significance of results and what they have learnt about the methodology of research. Well edited, focused writing and presentation, where the key decisions, developments, lines of argument and salient research are explained succinctly, is preferable to unstructured writing and presentation where little attempt to select or edit material has been made.

It is important to recognise that there are many different formats that a student could use to present their work and it is important that students think carefully about the suitability of the format in relation to the target audience. Both verbal and written forms of communication should be appropriate to the audience, both in terms of the nature and level of material they use and in terms of length. Students should be guided to produce research that gives a succinct account of the main arguments or developments from their project. If a verbal presentation is the chosen format, the question and answer session should address issues raised by the presentation, but also give students an opportunity to review their work.

Students are to submit as evidence for the unit in addition to their project findings, the ***research proposal and ethics form***. The research proposal sets out the plan for how the students will achieve the intended research objective and shows whether the

objective will be feasible, ethical and achievable in the time scale. It sets out how secondary research supports the research objective, how the research will be conducted, how the research will be evaluated**.** Students will need to gain ethical approval before commencing their research, this will be discussed with the tutor during the research proposal.

4 Employer engagement

It is advisable that centres look at the Pearson-set Assignment as an appropriate unit to embed employer engagement, although this is not a mandatory requirement. Developing and establishing links with employers enhances the teaching and learning experience and improves students' employability. Where possible, identifying links with employers as part of the delivery of the Pearson- set Assignment could lead to enhancing and supporting student learning. Real-life projects provide students with the opportunity to develop and acquire appropriate skills, knowledge and expertise required by employers.

5 Sharing of good practice

An appointed External Examiner (EE) for the centre will ask to sample the Pearson -set assignment briefs for review as part of the remote sampling request. Although this is not a mandatory requirement for centres we strongly advise that centres seek guidance and support from their EE on the Pearson-set assignment. The EE may also include the Pearson-set units in the centre visit sample of student work.

The EE will review and identify exemplars in all aspects of good practice. Good practice will focus on current themes that align to QAA Higher Education Reviews:

- Innovation
- Digital literacy
- Student employability and entrepreneurial skills
- Employer engagement
- Quality of assessment feedback.

6 Assignment guidance / Useful links

Suggested resources and links that centres may find useful are shown below. Centres should choose those resources that are relevant for localised use and complement these with additional resources to support independent research into the chosen topic.

Useful resources for underlying principles, examples of articles and webinars on the theme:

Resource Number	Type of Resource	Resource Titles	Links
1	Article	What is Network Intrusion? Definition, Detection, and Prevention	https://www.zenarmor.com/docs/network-security-tutorials/what-is-network-intrusion
2	Article	A guide to ransomware	https://www.ncsc.gov.uk/ransomware/home
3	Article	What is AI for cybersecurity	https://www.microsoft.com/en-gb/security/business/security-101
4	Article	What is Ethical Hacking?	https://www.itgovernance.co.uk/ethical-hacking
5	Article	Internet of Things and Cybersecurity: Emerging Trends, Challenges, and Solutions	https://deviceauthority.com/internet-of-things-and-cybersecurity-emerging-trends-challenges-and-solutions/
6	Article	Multi-factor authentication for your corporate online services	https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services/why-mfa-matters
7	Article	Multifactor Authentication	https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication
8	Article	The cloud security principles	https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles
9	Article	Virtualisation security design principles	https://www.ncsc.gov.uk/collection/cyber-security-design-principles/virtualisation-security-design-principles

10	Article	What Is a Social Engineering Attack?	https://www.cisco.com/c/en_uk/products/security/what-is-social-engineering.html
11	Article	What Is A Deepfake?	https://www.fortinet.com/uk/resources/cyberglossary/deepfake
12	Article	Critical infrastructure and cybersecurity	https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en
13	Article	Cyber security risk management framework	https://www.ncsc.gov.uk/collection/risk-management/cyber-security-risk-management-framework
14	Article	What is mobile security?	https://www.ibm.com/topics/mobile-security
15	Article	Protect and modernize your org with a Zero Trust strategy	https://www.microsoft.com/en-gb/security/business/zero-trust
16	blog	Ransomware Blog	https://ransomware.org/blog/
17	Blog	AI and cyber security: what you need to know	https://www.ncsc.gov.uk/guidance/ai-and-cyber-security-what-you-need-to-know
18	Blog	The State of AI in Cybersecurity: The Impact of AI on Cybersecurity Solutions	https://darktrace.com/blog/the-state-of-ai-in-cybersecurity-the-impact-of-ai-on-cybersecurity-solutions
19	Blog	Ethical Hacking Blog	https://www.ethicalhackingblog.com/
20	Blog	IoT Security Foundation Blog	https://iotsecurityfoundation.org/blog/
21	Blog	Global Institute of Cyber Security and Ethical Hacking	https://gicseh.com/blog.php
22	Blog	Coud computing and Cybersecurity: everything you need to know	https://gca.isa.org/isa-global-cybersecurity-alliance-blog-article-submission-guidelines

23	Blog	The Evolution of Cyber Threats: Past, Present and Future	https://online.yu.edu/katz/blog/the-evolution-of-cyber-threats
24	Blog	Mobile Security	https://www.mcafee.com/blogs/mobile-security/
25	Book	Guide to Computer Network Security	https://doi.org/10.1007/978-3-031-47549-8
26	Book	Computer Network Security	https://doi.org/10.1007/978-3-540-79698-5
27	Book	Cryptography and Network Security: Principles and Practice	https://doi.org/10.1080/19393555.2014.900834
28	Book	Ransomware Evolution	https://www.routledge.com/Ransomware-Evolution/Ahmed/p/book/9781003469506
29	Book	Ransomware and Cybercrime	https://doi.org/10.1201/9781003278214
30	Book	Artificial Intelligence and Cybersecurity	DOI https://doi.org/10.1007/978-3-031-15030-2

Additional materials
Pearson-set Report 2018–2019: https://hnglobal.highernationals.com/sites/default/files/Pearson-set-Report-2018-2019-final.pdf
Training Video for the RQF BTEC Higher Nationals Pearson-set Assignments: https://youtu.be/FkQi_l78_tw

The Pearson-set Assignment Guidance for Unit 16: Computing Research Project should be read in conjunction with the theme release. It provides advice and guidance for both tutors and students.

For any further additional support or queries regarding this document, please email btecdelivery@pearson.com

March 2025

For information about Pearson Qualifications, including Pearson Edexcel, BTEC and LCCI qualifications visit qualifications.pearson.com

Pearson Education Limited. Registered in England and Wales No. 872828
Registered Office: 80 Strand, London WC2R 0RL.

VAT Reg No GB 278 537121