The Marches
Centre for Cyber Security

A collaboration between

the University of Wolverhampton &

Herefordshire Council

5th December 2018

Contents:

Appendices:

1: EXECUTIVE OVERVIEW

As part of a plan for investment in Cyber Security, this business case outlines the proposed development of a unique Centre for Cyber Security on the Hereford Enterprise Zone to date. Such a Centre will ensure the University is able to capitalise on the growth in the cyber security sector by acting as a hub for cyber related research and development with access to world leading partners in the region, business start-ups, as well as larger businesses and engagement in a region recognized by the government as the focus for future growth and investment in cyber related activities in the United Kingdom.

The £9 million facility comprising office space/secure training rooms/laboratories, incubation space for start-up companies, advanced facilities for cyber space research and development and the commercialisation of intellectual property will be a joint venture between the University of Wolverhampton and Herefordshire Council. It will provide a route to market for the research capability of the University in the field of cyber security as well as employment opportunities for University graduates.

The planned location of the Marches Centre for Cyber Security is in a region of significant importance in the cyber eco-system. As such, the University of Wolverhampton will have a presence in the heart of regional and international cyber business development, driving innovation, job creation and investment alongside upskilling and leading edge research which will:

- Increase student recruitment through association with a world class centre in the field of cyber security and delivery of industry accredited training courses
- Create industry accredited curriculum in cyber disciplines at undergraduate and postgraduate levels
- Increase collaboration with national stakeholders
- Increase the number of Knowledge Transfer Partnerships and the number of co-funded Industrial PhDs in STEM subjects
- Develop cyber related student projects at all levels to align with industry needs to gain essential practical skills and experience for future graduate level careers
- Create unique, mutually beneficial, commercial relationships with global industry leaders in the field of Cyber Security

The proposed Centre for Cyber Security aligns with the University of Wolverhampton ‘Our Vision, Your Opportunity’ strategy which aims to enhance the experience for students, increase the skills-base in the region, create jobs and drive economic regeneration as well as provide a direct response to the Industrial Strategy and changing perspectives of Higher Education in relation to student expectations.

Herefordshire Council will be a partner in the development which will include contributing the land on the Hereford Enterprise Zone for the Centre as part of a long term lease as well as loan funding. The University has been successful in securing £4M of public sector capital grant funding towards the total build cost of £9M to develop this new facility as well as revenue funding of £270K. A request has been made to Herefordshire Council for a loan of £3.5M in the project. The University has approved a loan of £1.5M which will ensure the Centre sits at the forefront of Cyber research and industry collaboration.

2: BACKGROUND

The growth of the internet, or cyberspace, has impacted profoundly on everyday life and the global economy. By enabling people to exchange knowledge and ideas all over the world, the internet has contributed to a more open society and greater freedom of speech. It has transformed the conduct of business and opened up new markets. The internet is also making governments more accountable and transparent and is changing the way they deliver public services.

The internet has evolved from initial experiments to link computer systems in the US in the 1960s, to the global interconnected network of systems and information that it is today. Commercial investment and technical innovation have driven these changes. Whilst nobody controls the internet and no one person owns it, 80% of the internet lies in the private sector. It is impossible to predict how people will use the internet in the future. With digital information growing, combined with new technologies, government, industry, the public are likely to depend increasingly on the internet. Approximately three billion people are now using the internet and it was not designed with security in mind.

In a single month, the UK spends an estimated £10.7 billion shopping online and one eighth of the UK's GDP comes from the digital economy, which is the highest currently in the G20. The UK's digital industries grew two and a half times more quickly than the economy as a whole over the last 15 years and the UK has the highest percentage of individual internet usage of any G7 economy. A secure internet is therefore vital for the UK's economic prosperity and to support government plans to make all public services digital. Future skills and employment opportunities for University graduates will result, in many as yet unknown ways.

'Cyberspace' is the term used to describe the electronic medium of digital networks used to store, modify and communicate information. It includes the internet as well as other information systems that support businesses, infrastructure and services.

Cyberspace lies at the heart of modern society; it impacts our personal lives, our businesses and our essential services. A secure online environment is essential to the Government, which is providing an ever-increasing number of online services to general public and businesses as part of a major digital services transformation programme. The ability to conduct online transactions securely is central to the delivery of public and commercial services and communications.

Cyber security affects both the public and the private sector and spans a broad range of issues related to national security, whether through terrorism, crime or state and industrial espionage. Cybercrime and data protection, whether relating to theft, hacking or denial of service to vital systems, has become a fact of life. The risk of industrial cyber espionage, in which one company makes active attacks on another, through cyberspace, to acquire high value information is also very real.

A wide range of hostile actors use cyber space to target the UK. They include foreign states, criminals, ‘hacktivist’ groups and terrorists. The resources and capabilities of such actors vary. Foreign states are generally equipped to conduct the most damaging cyber espionage and computer network attacks.

Hostile actors conducting cyber espionage can target the government, military, business and the public. They use computer networks, for example, to steal large volumes of sensitive data undetected. This might include intellectual property, research and development projects, strategic data on a company's merger and acquisition plans, electoral information or any other information that the owner might want to protect.

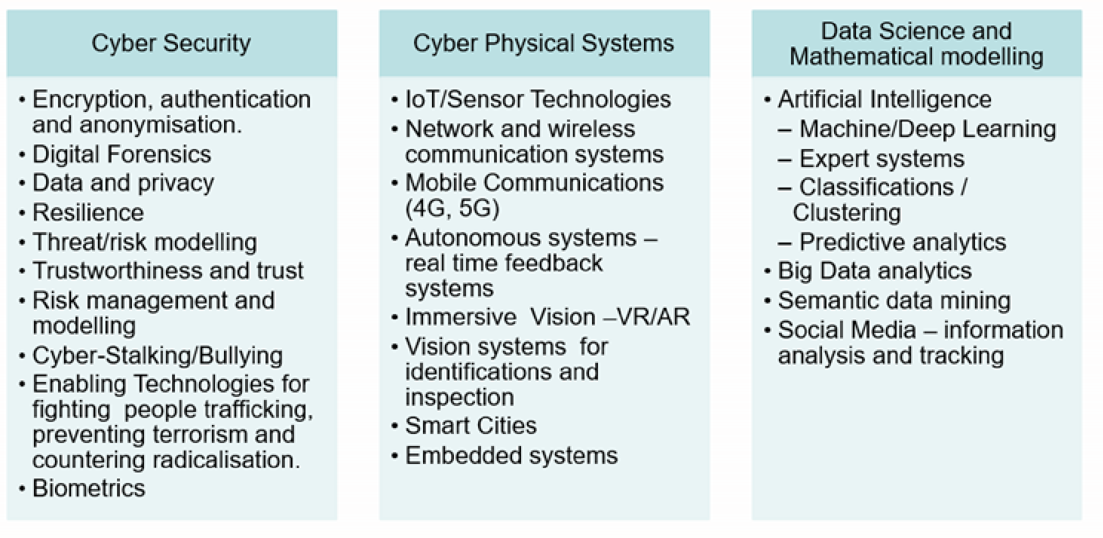
Cyber espionage should be viewed as an extension of traditional espionage. It allows a hostile actor to steal information remotely, cheaply, on an industrial scale and with relatively little risk to the attacker. Hostile actors can also use malicious software (or malware) to disrupt and damage cyber infrastructure. This can range from taking a website offline to manipulating industrial process command and control systems.

Cyberattacks are easy and cheap to perpetrate compared with traditional crime and attackers can easily evade prosecution by being in countries that will not arrest them. Consequently, tackling crime using the internet is a major challenge and one that the UK will need to support. Serious organised crime has developed an internet-based black market for criminals, which sells stolen identity information and software products to launch cyberattacks as well as technical support for cybercrime. The threat to cyber security is persistent and constantly evolving. The covert nature of the threats however, means that people often underestimate the risk to business, government and the public. Cybercrime currently costs the UK between £18 billion and £27 billion a year. 65% of all large UK companies reported a breach in the last year and the media in the UK is full of painful stories of small businesses struggling to survive and maintain the confidence of their customers after a ransomware attack. For UK businesses, it is no longer an issue of whether they will be attacked - the reality is that organisations now need to focus their efforts on determining when the attack took place and identifying that they fell victim to the cyber threat in the first place. Consequently, business, government and the public must be aware of it and be able to resist the threat of cyberattack. Since 2011 the cyber security sector has grown from £10 billion to over £17 billion and employs 100,000 people. Cyber security exports were at £1.47 billion in 2014, up 35% since 2012 and on-track to rise to £2 billion in 2018.

3: THE UNIVERSITY OF WOLVERHAMPTON AND CYBER SECURITY

RESEARCH FOCUS

To support the growth in cyber related research activities and address threats in cyberspace through high quality impactful research and knowledge transfer with businesses at the University of Wolverhampton, the Wolverhampton Cyber Research Institute (WCRI) was established in 2017. This institute brings together under one umbrella, a number of research teams from the School of Mathematics and Computer Science within the Faculty of Science and Engineering and currently comprises 24 academic staff who undertake research within the three main research pillars shown below in Figure 1.



Cyber Security	Cyber Physical Systems	Data Science and Mathematical modelling
• Encryption, authentication and anonymisation. • Digital Forensics • Data and privacy • Resilience • Threat/risk modelling • Trustworthiness and trust • Risk management and modelling • Cyber-Stalking/Bullying • Enabling Technologies for fighting people trafficking, preventing terrorism and countering radicalisation. • Biometrics	• IoT/Sensor Technologies • Network and wireless communication systems • Mobile Communications (4G, 5G) • Autonomous systems – real time feedback systems • Immersive Vision –VR/AR • Vision systems for identifications and inspection • Smart Cities • Embedded systems	• Artificial Intelligence – Machine/Deep Learning – Expert systems – Classifications / Clustering – Predictive analytics • Big Data analytics • Semantic data mining • Social Media – information analysis and tracking

Figure 1: WCRI Research Pillars

The Vision and Mission of the institute are as follows:

- *Vision* – The Wolverhampton Cyber Research Institute aims to become a world leading multi-disciplinary Cyber Research Centre of Excellence.

- *Mission* – Our mission is to undertake world leading research in innovative cyber solutions, provide a platform to facilitate long term academic-industry collaboration and to influence cyber policy and decision making that ensures the protection of businesses and individuals in cyberspace.

The objectives of the institute are to:

- Carry out cross disciplinary internationally leading research in the cyber domain (leading to a successful REF submission)
- Develop collaborations for undertaking high quality research, knowledge transfer and business enterprise support with partners both within the UK and internationally

- Organise, facilitate and support the development of cybersecurity on a global scale
- Develop research informed high quality academic/vocational educational and training programmes

The research institute is now rapidly expanding following the recruitment of five new members of academic staff in 2018, who bring a wealth of experience and expertise. The overarching theme of the institute's research focus is on the '*Security of Critical National Infrastructure (CNI)'.* Research is conducted into various security aspects of CNI including power networks, water networks, transport systems, NHS, etc. which are all central to the ability of modern societies to function and where a major attack on any one would shut down the country. Whilst future CNI systems aim to use internet communication to provide efficient control and better utilisation of resources, it will leave them vulnerable to various security attacks. The WCRI team investigates the use of multidisciplinary concepts to develop innovative end-to-end security solutions to close the loop of prevention, detection and recovery from security attacks, helping to improve the security, resilience and reliability of the critical national infrastructure and help reduce societal and environmental impact of security attacks. In particular, this research focuses on the following applications:

- Secure Healthcare
  - Secure exchange of patient information, secure electronic devices, secure intensive care, etc.
- Secure Transport
  - Automotive: Vehicular communication, secure drive by wire systems, secure self-driving cars, etc.
  - Aviation: Secure Air traffic management, secure aeronautical communications, secure fly-by-wire, secure airports, etc.
  - Secure Space - Satellite networks / Space stations
- Secure infrastructure for sustainable cities
  - Security for smart power grids: secure smart grid communications, privacy of energy usage, etc.

The focus of the research has been carefully and strategically chosen and reflects:

- The research expertise and experience of the academic staff members
- The publication of several recent government reports that highlight the need for protecting the UK's CNI
- Feedback received by various prospective industry collaborators

UNIVERSITY BUSINESS ENGAGEMENT

The University is a major provider of knowledge exchange and innovation services with business and the wider community, regionally, nationally and more recently internationally. It is recognised as being at the forefront of the Higher Education sector in working with businesses demonstrated by the number of knowledge transfer activities delivered that include KTP (Knowledge Transfer Partnerships) and other similar knowledge exchange and enterprise projects. In addition, the University is delivering new enterprise activities in the Black Country, Telford & Wrekin, Shropshire, Stafford, Herefordshire and the Wyre Forest.

The University has a number of centres that provide services to individuals and businesses for business start-up and incubation including: an ICT business incubator (e-Innovation Centre), business grow-on space (Business and Technology Centre), a Creative Industries business incubator (SP/ARK), a Student / Graduate business incubator (SP/ACE) as well as facilitating University of Wolverhampton graduate start-up businesses through the Student Placements Programme for Entrepreneurs in Education (SPEED).

The University's knowledge transfer, business innovation and incubation activities are delivered primarily from the University of Wolverhampton Science Park, Telford Innovation Campus, Hereford Enterprise Zone and more recently the Wyre Forest.

University business engagement activities have been strengthened through the colocation of the University's Business Solutions Centres and the-National Growth Hub initiative across the Black Country and the Marches, including Telford & Wrekin and Hereford whereby University staff work in partnership with their public sector partners to deliver business support services.

The business support services in Hereford are delivered through a new Business Solutions Centre which opened in 2015, on Skylon Park – the Enterprise Zone in Hereford.

The Centre offers businesses:

- Support services to help improve business competitiveness
- Networking events from live budget debates, to workshops and seminars covering sources of funding, pensions and digital marketing
- Incubation space for start-up/young businesses; providing space plus opportunity to network and easily access support and funding
- Event space, meeting rooms and event management

Skylon Park has a strong focus on the Defence and Security sector building on the deep rooted association that Hereford has with the UK Special Forces as the base of the SAS, a globally recognised organisation in the Defence Sector. The existence of other key sites, QinetiQ in Malvern and GCHQ in Cheltenham, form a local cluster of strategic sites in 'quiet' locations from which Skylon Park draws. In total, defence and security businesses employ approximately 2,600 people across the Marches (ranging from manufacturers of military vehicles, weapons, explosives, systems and technologies, private security, security systems and investigation).

There is an inevitable emergence of businesses in the security sector in Herefordshire. It is already the location for over 200 companies in the sector, many of which have been set up by ex-military personnel who have engaged in the Special Forces supply chain utilising their specialist skills to maximise business opportunities. Skylon Park is the only Enterprise Zone in the country to focus on the defence and security sector, where there are plans to build on the base of 70 plus small businesses operating locally in this market.

Cyber security however reaches beyond the defence and securities industry and is of growing interest to all SMEs as the associated costs and risks of protecting on-line assets grow. Many businesses are not fully embracing the productivity benefits offered by the digital agenda and are not effectively managing the risks they have taken on. This means cyber-security markets not only have huge growth potential but also have significant technological requirements to research, innovate, test, develop and demonstrate its products and services. The capital costs involved in research and development however, alongside the commercial risks for business deter many innovators and entrepreneurs from developing new businesses.

As described above, the UK Government has put a great deal of emphasis on cyber security and has invested £1.9 billion in protecting the UK from cyber-attack and developing capabilities in cyberspace. It has committed to a new National Cyber Security Centre, three Research Institutes, 13 Academic Centres of Excellence in Cyber Security Research and two Centres of Doctoral Training (offering 100 PhDs in cyber security by 2019). Cyber security reaches beyond the defence and securities industry and is of growing interest to all SMEs as the associated costs and risks of protecting on-line assets grow. The Marches, through the natural clustering of security and defence businesses in Herefordshire, is well placed to seize this opportunity to secure a larger share of this market as the Government commits more investment and global opportunities grow.

4: PROPOSED DEVELOPMENT OF A CENTRE FOR CYBER SECURITY

It is proposed to develop a Centre for Cyber Security located on the Hereford Enterprise Zone, as a joint venture with Herefordshire Council. The proposed site is strategically located on an Enterprise Zone at the heart of the security and defence sector in the Marches and will form part of a national '***Cyber Triangle'*** with GCHQ Cheltenham and the Government Cyber Centre in Newport, South Wales. It will be an anchor building generating new research and short course opportunities that will feed into training and education in industry and within the University. This will enhance the student experience through the provision of research informed curriculum, application of applied research and knowledge transfer partnerships.

Furthermore the Centre will:

- stimulate a base of SMEs engaged in cyber-security solutions
- drive up levels of innovation activity in the field of cyber-security and industry links for digitally orientated researchers
- generate a step change in commercial income activities
- improve insight on cyber-security challenges and opportunities for SMEs across the Marches that as a consequence provide insight to undergraduate and post graduate students.

Through the provision of the following spaces:

- office/workshops/laboratories for cyber related tenant companies and incubation space for start-up companies
- advanced facilities for the University's Wolverhampton Cyber Research Institute and partners to undertake cyber space research and commercialisation of intellectual property
- secure training rooms for the delivery of Industrial and University short courses
- remote access that can feed expertise into wider educational programmes

all co-located under one roof in a specialist facility which will be a focal point for cyber-security activity and defence /security related businesses and associated R&D.

The centre will provide innovation workspace for small and start-up businesses to operate from. These facilities will provide ready access to consultancy support from the University and shared facilities including lab space and training rooms. The combination of support, facilities and co-location with potential collaborators will significantly enhance the environment for investment and enterprise. It will contain specialist facilities for the cyber sector including server space, very high speed broadband, as well as R&D lab space for the University's Wolverhampton Cyber

Research Institute to collaborate with business partners. The physical fabric of the building will offer the high levels of security for data transmission and storage which will ensure the Enterprise Zone attracts a growing base of cyber-related businesses and activity.

The building will provide users with access to space and support, connections, knowledge, experience and investment through:

- Over 1,000m² of R&D floor space for 3 cyber laboratories, providing new laboratory and testing facilities for researchers in this area.
- More than 1,500m² of employment space for 16 cyber security business incubator units, 2 workshops and 3 high security meeting rooms
- 250m² of high quality secure business training floor space

The fabric of the building will contain a physical security firewall between all major elements of the building and a secure server room. A series of internal and external images of the proposed building are shown in Appendix 1 and a schedule for the development of the project is shown in Appendix 2.

It is proposed that the Centre will be a joint venture between the University of Wolverhampton and Herefordshire Council. The planned activities to be undertaken within the Centre for Cyber Security will comprise:

- Research & Knowledge Transfer
- Incubator and tenant companies
- Training programmes delivery

- Research

The research undertaken by the University's Wolverhampton Cyber Research Institute and partners will be instrumental in developing intellectual property and informing undergraduate curriculum development.

- Incubator and tenant companies

The Centre for Cyber Security will provide a home for established cyber businesses as well as a space for the next generation of cyber start-up businesses. The businesses will have access to workshops, meeting rooms, offices and laboratories and will be able to gain access to world-class expertise and leading edge technological resources to allow them to expand capability, improve ideas and devise cutting-edge products to outpace current and emerging threats. It will create a 'honeypot' where these businesses will thrive and support each other.

- <u>Training programmes</u>

The digital economy together with the cyber security sector is quickly expanding and its stakeholders need to keep up with its growth by recruiting and developing the talent pipeline this requires. In 2016 however, 85% of IT decision makers felt that there was a shortage of cyber skills in the UK and that by 2019 there would be a projected shortfall of 1.5 million[1] cyber trained staff. A recent report from Indeed put the UK in second place globally in terms of demand for cyber-security professionals but only 12% of the cyber-security workforce is under the age of 35, indicating a decreasing pipeline of talent coming into the industry.

By failing to recruit new talent, companies are left unprotected and vulnerable to the growing wave of cyber-crime. Companies need short, condensed and hands on courses that can quickly address their immediate needs to deal with emerging threats. Short training courses, accredited by a variety of professional bodies have proved to be highly successful and this market segment can be exploited to address an arising market failure. Upskilling an IT professional for example, to become a Cyber professional will require them to undertake a number of short courses (3 to 5 days in duration).

5: OPERATIONAL MODEL AND GOVERNANCE

It is proposed that a subsidiary company of the University of Wolverhampton be incorporated and in conjunction with Herefordshire Council, secure, develop and operate the Centre for Cyber Security which will be developed on the Hereford Enterprise Zone.

Identification of options and advice have been taken from external specialists on the formation of the joint venture company as well as on current State Aid matters. The proposed model for the Joint Venture is a model which reflects the joint venture between the University and Wolverhampton City Council in operating the University of Wolverhampton Science Park which has been in operation for more than 20 years.

6: THE FINANCIAL CASE

The total cost of the build project is £9M with an additional cost of land of £0.5M to be leased from Herefordshire Council. A detailed and robust assessment of the building design and costings has been conducted since mid-2017, including discussions with contractors. The current cost plan demonstrates that the project can be delivered within the budget.

Description		Year 0 2018/19	Year 1 2019/20	Year 2 2020/21	Year 3 2021/22	Year 4 2022/23	Year 5 2023/24	Year 6 2024/25	Year 7 2025/26
		£	£	£	£	£	£	£	£
Income - Total		**220,500**	**1,154,000**	**2,285,620**	**2,977,390**	**3,784,910**	**4,215,280**	**4,207,830**	**4,664,560**
Expenditure - Total		**94,320**	**991,381**	**1,759,704**	**2,179,437**	**2,991,741**	**3,126,697**	**3,471,008**	**3,692,640**
Surplus / Deficit		126,180	162,619	525,916	797,953	793,169	1,088,583	736,822	971,920
Depreciation Charge			100,000	200,000	200,000	200,000	200,000	200,000	200,000
Increase/Decrease in Cash		126,180	262,619	725,916	997,953	993,169	1,288,583	936,822	1,171,920
Cumulative Cash			388,799	988,535	1,986,488	2,979,657	4,268,240	5,205,062	6,376,982

7: MANAGEMENT OF THE CONSTRUCTION PHASE

A Project Board was established in February 2017 to oversee the planning and design of the proposed Centre for Cyber Security to RIBA Stage 3. The Board meets monthly to oversee progress and is chaired by Deputy Vice-Chancellor Professor Ian Oakes with representation from the Faculty of Science & Engineering, the Department of Computer Science, Estates and Facilities, Procurement, Project Support Office, Business Solutions and Finance along with the following external members:

- Project Manager and Cost Consultant
- Architect
- M&E Engineer
- Structural Engineer
- Chief Executive of Hereford Enterprise Zone

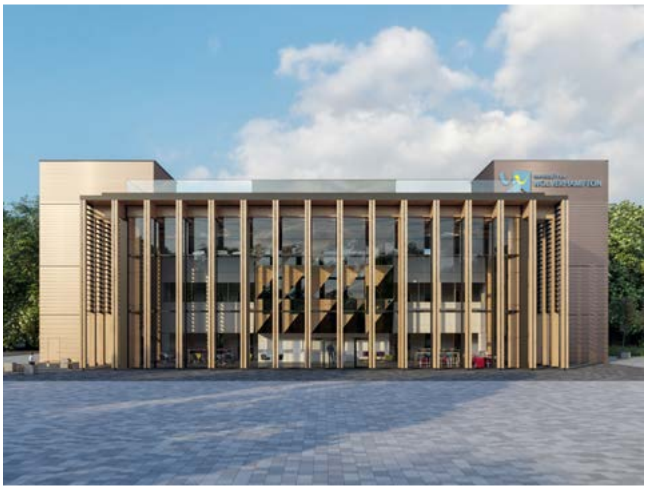
The Project Board will manage the construction of the building, reporting into the Governors Estates Sub-Committee to provide Governor oversight of the project and determine items necessary for escalation to the Planning and Resources Committee and/or the Board of Governors.

8: CONCLUSION AND RECOMMENDATION

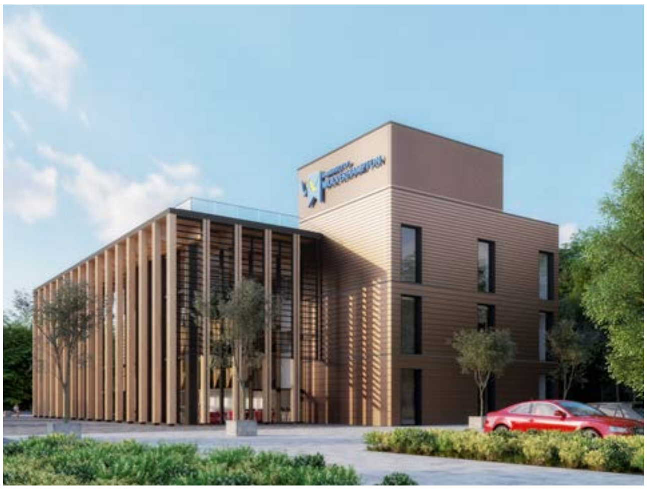
The ambition of the University and Herefordshire Council to create a Centre for Cyber Security on the Hereford Enterprise Zone, will capitalise on the growth in the cyber security sector. The proposed Centre, located in the ‘national cyber triangle’, will bring about growth in research, impact, income generation and reputation and provide a strong link between cyber businesses, research and development and employment opportunities in this field.

It is recommended that both partners support the proposal.

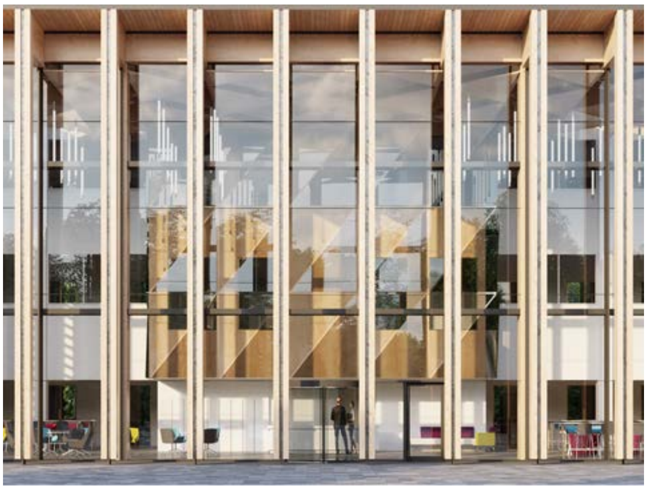
APPENDIX 1 – PROPOSED INTERNAL & EXTERNAL IMAGES



Front elevation



Side elevation



Front of reception

Internal view of reception

Internal view of reception

Tenant office

TRAINING ROOM

Training room

Cyber range

Schedule of accommodation

Space	Room Occupancy	Total Area M^2
Forensic Laboratories	4	40
Cyber-range	2	80
2P Cyber Tenant Unit	2	96
4P Cyber Tenant Unit	4	128
6P cyber Tenant Unit	6	288
Training Space	30	96
Innovation Sand Pit	12	36
Communal Refreshment Area		96
Reception Area	2	20
Visitors Meeting Room	6	12
IT Technician Office & Workshop	1	20
Staff Offices	1	15
Grand total		2,072 M^2

APPENDIX 2 – PROPOSED SCHEDULE

January 2017- October 2017	Planning and design (completed)
October 2017	Planning Consent (completed)
October 2017- December 2017	Tender review (completed)
July 2018	Stage 2 design (completed)
December 2018	Issue of contracts
January 2019	Mobilisation on site
February 2019	Building construction
July 2019	First fit commencing
September 2019	Second fit commencing
March 2020	Building completion
April 2020 – June 2020	Equipment installation
June 2020	Occupation
March 2021	Completion of defects liability period