Cambridge Assessment International Education

Cambridge Pre-U

GLOBAL PERSPECTIVES (SHORT COURSE) **1340/01**

Paper 1 Written Paper **May/June 2022**

INSERT **1 hour 30 minutes**

INFORMATION

- This insert contains all the resources referred to in the questions.
- You may annotate this insert and use the blank spaces for planning. **Do not write your answers** on the insert.

This syllabus is regulated for use in England, Wales and Northern Ireland as a Cambridge International Level 3 Pre-U Certificate.

This document has **4** pages. Any blank pages are indicated.

DC (CE) 310682

[Turn over

The documents below consider issues related to incorporating technology into buildings. Read them **both** in order to answer **all** the questions on the paper.

Document 1: adapted from *How AI Is Making Buildings Smart And Intelligent*, written by Naveen Joshi. The article was published on Forbes.com in 2019. The author was Founder and CEO of Allerin, which develops engineering and technology solutions focused on customer experiences.

Smart buildings are more than just four walls and a roof.

Content removed due to copyright restrictions.

Now that's exactly what sustainable development is all about, isn't it?

Document 2: adapted from *Why cyber criminals are targeting smart buildings*, written by Carey van Vlaanderen in 2019. Published online on News 24 South Africa. The author was CEO at ESET South Africa.

Smart buildings use Building Automation Systems (BAS) to control their environments for the comfort, health and productivity of the people inside them. With the arrival of the Internet of Things (IoT), smart buildings are transformed. Using information from smart sensors, the technology analyses, predicts, diagnoses and maintains the environment. Temperature, lighting, security cameras, elevators, parking and water management are just some of the automatable services supported by this technology.

A smart building in Las Vegas illustrates the possibilities. Two years ago, they installed an automatic smart system to ensure the air conditioning only turns on when people are present. This system saved US$2m during the first year after installation, due to the reduction in energy consumption. Marriott Hotels has introduced a similar system across its entire chain and expects to achieve an estimated US$9.9m in energy savings. Another example is a supermarket in the UK, where they installed a smart system in the parking lot. This generates kinetic energy from the movement of cars passing through and uses that energy to power the checkouts.

At first glance these smart buildings seem risk-free. However, IoT devices are manufactured by different suppliers, who may not pay attention to security considerations. Smart networks may be connected to the internet and that is where the risk is. Tools, such as Shodan, allow anybody to discover vulnerable and/or unsecured IoT devices connected to the internet, with information that could be used to get access to them. This means that someone could take control of a BAS after finding it through a search.

In February 2019, around 35 000 building automation systems worldwide appeared in Shodan. Using Shodan, criminals can find the IP address of an automation system, copy it into the address bar of a web browser, and bring up an interface to gain access. If the system uses a default username and password, the attacker can easily access the system-monitoring panel in the smart building.

Once attackers have access, they can monitor how the air conditioning or heating works. They can call up pretending to be from the maintenance company. They say they are going to send a technician and they will need remote access to the server, allowing them to control the building. Once they have control, they can alter the building's heating or air conditioning or adjust any of the other automated systems. Then they can demand payment of a ransom, using an anonymous system such as cryptocurrency, in exchange for not shutting the building down. This kind of attack is called siegeware. Cybercriminals are already carrying out siegeware attacks to make money when they have the opportunity.

In conclusion, the low cost of IoT devices for buildings and the advances of technology for building automation systems are transforming building management. Automation and the use of smart devices give a building's users more comfort and use resources more efficiently. However, they bring increased security risks. As a result, the possibility of a cybercriminal launching a ransomware attack on a smart building is already a reality.

BLANK PAGE