Questions on the Draft Cybercrime (Jersey) Law 201- ("the Law")

1. Article 19 – How is "in a timely manner" defined? What is the proposed timescale?

The phrase 'timely manner' is a standard in legislation where the precise timings of the required action depend on the facts and circumstances of the case. Courts have a wide discretion in interpreting this phrase and will seek to do so fairly.

2. Page 20 Section 5D (4) – To what level can a company disclose a request for information to others within the company for the purposes of complying with the request?

If a request has been made to the company itself then disclosure to individuals within that company would seem to be within the terms of the request and so should not be an issue.

3. Page 21 Section 3(2)1(A) (C) – Does this refer to cloud services and or cloud storage?

Yes.

4. Article 5A (i) - What consideration has been given to tools that may be "dual use"? (i.e. can be used for both legitimate and illegal purposes) .

The focus of Article 5A(1) is a person's intention that, in making, adapting, supplying or offering the relevant article, it will be used to commit or assist in the commission of an offence under Article 2 or Article 5.

5. Article 5A (i) – Is it the intention of the law to hold someone accountable for the actions of a second party, and what safeguards are in place to protect legitimate businesses who may sell duel use items? (Is there a way of determining that the seller did not know the intentions of the second party?)

See point 4 above. Were there to be some question that a "dual use item" was used in the commission of an offence, that case would be decided on its own facts as to whether those involved intended that the item would be used to commit an offence under the Law. (see also Article 5A(2) which says that a person is guilty of an offence if *"he or she supplies or offers to supply any article in the commission of an offence under Article 2 or 5".)*

6. Article 5A (i) – Could security professionals be effective charged under the draft law subject to intent?

Anyone can be charged under the Law if there is evidence that their intention has been to commit an offence.

7. Article 5A (i) – What consideration has been given as to whether this draft law will dissuade people from teaching and learning in this area?

Legislation equivalent to the Law is in place in any jurisdictions including the UK, so practitioners should have a good understanding of its implications. The central element of the relevant offences is intent, and so educational activities should be unaffected.

8. Computer Misuse (Jersey) law 1995 – As the draft law does not define computer, what consideration has been given to the types of devices that this would include?

The Crown Prosecution Service in the UK has published guidance on the UK Computer Misuse Act, which is similar in purpose and approach to the 1995 Law. It advises that the Act *"deliberately does not define what is meant by a 'computer', to allow for technological development. In DPP v McKeown and, DPP v Jones [1997] 2 Cr App R 155 HL, Lord Hoffman defined computer as* 'a device for storing, processing and retrieving information'*, this means that a mobile smartphone or personal tablet device could also be defined as a computer in the same way as a traditional 'desk-top' computer or 'PC'.*

Similarly, in Jersey, allowing the Courts to define 'computer' in this manner is intended to allow the 1995 Law to survive unanticipated changes in technology.

9. Computer Misuse (Jersey) law 1995 – Is the law future proofed to include smart devices (i.e. Amazon Alexa, Kettles etc.)

Yes, for the reasons explained at 8 above, above, these devices would be within the scope of the Law.

10. Regulation of Investigatory Powers (Jersey) Law 2005 Article 42F – What process will be followed when requesting a key for a device from an individual?

The UK Home Office has published a Revised Code of Practice on the Investigation of Protected Electronic Information, dated August 2018. This sets out the process that must be followed in those circumstances by UK authorities exercising powers under the UK Regulation of Investigatory Powers Act ("RIPA"). Post-amendment, our domestic Regulation of Investigatory Powers Law ("RIPL") will be functionally very similar to the UK legislation so there will be potential for SoJP to consider the relevant Home Office guidance as it does in other areas of police procedure.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742064/RIPA_Part_III_Code_of_Practice.pdf

11. Regulation of Investigatory Powers (Jersey) Law 2005 Article 27(A) – does this section of the law cater for operators using contractors or third parties to carry out work?

The Law as it amends RIPL does not expressly refer to contractors or third parties carrying out work. The current version of RIPL simply refers to "postal or telecommunications operators" as meaning "*a person who provides a postal service or telecommunications service*" (Article 24)). Where there is any question as to whether a notice and its contents (as given to a postal or telecommunications operator) is to be kept secret, Article 27A(8) is engaged. Here, a disclosure is defensible if it is made to the Commissioner or authorized – (a) by the Commissioner; (b) by the terms of the notice; (c) by or on behalf of the person who gave the notice; or (d) by or on behalf of a person who – (i) is in lawful possession of the protected information (within the meaning of Article 42A(1)) to which the notice relates, and (ii) came into possession of that information."

12. Is it intended for there to be any guidance around the work of security practitioners, especially training in this field and around ethical security?

Not specifically in Jersey, but comparable provisions have been in place in the UK for over 10 years so it is a reasonable assumption that most practitioners will have some understanding of the requirements.

13. What consideration has been given to the impact on someone's mental health if they are genuinely unable to remember an encryption password?

The offence of failure to comply with a notice (Article 42F) is only met when a person "knowingly" "fails to make the disclosure required by the giving of the notice and in accordance with the notice", such a test is fact-dependent in each case (Article 42f(3)). In corporate bodies, the notice might be addressed to multiple people, avoiding this issue.

14. Who is intended to be asked for access to systems within an organisation and what is the protocol for doing so?

In the context of a notice, Article 42B(5) requires that a senior officer of a body corporate shall be the recipient unless there is no such senior officer. Further, where more than one person is in possession of a key to any protected information (as employees of a firm), a notice may be given to any employee, unless there is a partner or more senior employee to whom it is reasonably practicable to give the notice.

15. Regulation of Investigatory Powers (Jersey) Law 2005 Article 27(A) – What is the intention of the law in relation to third party contractors?

See answer to 11 above.

16. Regulation of Investigatory Powers (Jersey) Law 2005 - What is meant by economic well-being of the Island when seeking grounds to investigate a device and seek access to it?

The relevant authority will have to convince a Court that an action is 'in the interests of the economic well-being of Jersey', and the Court will decide if this is a valid claim on the particular facts and circumstances of the case. The 'economic wellbeing of the country' is identified in the ECHR as a reasonable ground for states to take certain actions, and the UK's Regulation of Investigatory Powers Act 2000 contains the same provision.

17. Does this legislation offer futureproofing against technology such as Artificial Intelligence and the Internet of Things?

In respect of the 'Internet of Things', as per question 8, the two safeguards are a) the current definition of "computer", which is wide enough to capture any data storage device, and b) the capacity of the Courts to interpret 'computer' as needed. If a 'Thing' has sufficient capacity to be wifi enabled it is likely to be a 'computer' under the Law, and if it is not it must be controlled by something that is a 'computer'. Accordingly, unauthorised access to, for instance, an internet-enabled refrigerator will, prima facie, be a crime under the Law.

Regarding 'Artificial Intelligence', any AI with data storage capacity will be treated as a computer system. There may be significant questions around AI culpability and policing of AI generated activity, but these are wider questions for the justice system to consider.

18. Can the authorities demand a key to data that has been obtained unlawfully?

Yes.

19. What if decrypting a drive provides access to significant other information not related to the investigation? How will this be managed?

Sensitive information that does not relate to a criminal offence will be treated in complete confidence. Evidence that points to other offences will be dealt with in the normal manner and

may result in a prosecution for the relevant office. This is the case with evidence uncovered in physical searches, and is already the practice in relation to digital evidence. For instance, were a computer seized as part of an investigation into online grooming, and indecent images of children were discovered, then those images could result in a separate prosecution.