Comments on the Cybercrime Jersey law 201

2nd January 2019

Comments by:

Ricky Magalhaes (CISSP)

Comments on the Cybercrime Jersey law 201

Thank you for asking me to advise, comment and consult on the Cyber Law proposal for Jersey 201

I have reviewed the law and my comments are as follows:

Cyber Security is a vast and broad topic and there are many areas of depth and expertise that are difficult to fully understand and or be an expert in, over my 21 years of experience on the topic I am still learning but have a strong command of the topic and the below are my opinions and observations based on my perspective and exposure.

I trust you find them balanced and unbiased to reflect the best advice I can offer.

1. What provision is there in the law for people that need to have equipment and software to perform their work, so that they can test systems for vulnerability? This is not covered in anyway and criminalises the use and provision of such equipment. In Jersey currently there are more than 5 companies that provide cyber security services that test systems. The law in its current state criminalises some of these activities as there are no provisions for testing and the tools required to do so. (should there be a licence to test and have these tools?)
2. Under article 5A this article must be amended to reflect a workable solution: for instance, encrypting is required and as long as the police (law enforcement) have the access to legally intercept the protected information then this should be legal, as the article reads, everyone supplying a solution that restricts access is breaking the law, so Apple, Google, Facebook and Microsoft are all in contravention. This article needs more work to cover Jersey more comprehensively.
3. The above 5A article also keeps making references to device, this should be TCB (Trusted Computing Base) which is not limited to hardware, but includes software and firmware, in most cases its software in any event and the law as written does not cover this.
4. On page 8 reference is made to a person granting access to a system, what happens if the person forgets the credentials or is unable for legitimate reasons not able to grant access to the system, does this mean a penalty or 5 years prison sentence will be levied? This part of the law needs to be enforceable and there are potentials to plausible deniability and no provision has been made for this. If this is a real concern or likelihood it must be drafted into law that systems that contain information that maybe requested by the authorities should be secured in such a way as there is another way in like a backup password for security and legal reasons. (Technology has evolved today to the point where it's no longer trivial and not having a backup password will render the information unreadable)

Comments on the Cybercrime Jersey law 201

5. There are several areas in the law that are unclear on if there is sufficient evidence of or circumstances where there is cause for concern where search and seizure is required. The law does make provision for ECHR however there maybe circumstances where this part of the law will need to be reviewed and amended in defence of the greater population of Jersey. For instance, someone could argue that there is not enough evidence to search their computer and that it in contravention of their basic human right of respect for his privacy and family life. A clear process should be in place to allow for this to quickly be disputed and resolved for to allow for the search if there are mitigating circumstances.
6. The law refers to RIPL and that the warrant is valid for 3 months, in cybercrime this period is too short as data and evidence can be and is likely to be scattered many areas, it may take over 6 months to gather all the evidence and that will tax the Jersey law enforcement and the population if reissuance of warrants etc. this should reflect a more realistic timescale.
7. I understand the law is based on the UK law and the Budapest convention, however my recommendation is that definition of words be clearly articulated, for instance what unauthorised access means. This may not be clear enough to the lay.
8. On page13 where data comes into someone's possession when its encrypted and access is required, if someone that has the data does not have access this can be argued and there should be no penalty for not providing the key if you don't have it, in the way this is laid out this puts onus on Jersey Authorities and will be very challenging to prove.
9. The next paragraph does not make provision for expiring keys which will render the data useless. It should read the data needs to be kept for a period of X in Jersey to ensure the data can still be accessed.
10. Additionally, what is the definition of a computer? Does it encompass, mobile phones, IOT devices and any electronic machine that can compute? Including cars, sensors, drones etc? Most people will define computers as servers, desktops and laptops, this needs to be clear.

To answer the questions as per your letter on the 13th of December please see my responses below:

1. Whether what is being proposed is fit for purpose;

   The written law as suggested in the draft is better than the current Law and will give Jersey a modern and applicable law in line with European standards. My recommendation is that the definitions of key elements be clearly laid out as to avoid confusion and ambiguity as currently the draft has certain areas that lends itself to this.

2. Whether it will effectively assist Jersey in the fight against cybercrime;

   The law will assist in fighting against cybercrime in Jersey and jurations that also comply with the Budapest convention. I am unsure how you are able to enforce this new law in other regions and this still needs to be seen and tested.

3. What impact the law may have on information support and development;

   Having a law like this in Jersey will make Jersey a stronger jurisdiction, this will mean that we are no longer a soft target and now can prosecute if our computer resources are tampered with. The Law should however be further amended to cover all form of

computing like IOT devices, mobile phones, cameras and anything digital or have the capability to process and compute. This will further reinforce the law and protect Jersey and its citizens.

4. Whether you think any improvements or changes could be made to enhance the law.

   The following improvements additional to the observations above should be made

1. A closer look at Human Rights section to ensure there is a clear process by which law enforcement will follow when investigating anyone. Human rights must be upheld.
2. Define Data as an asset that can be stolen

Sincerely,

Ricky Magalhaes
CISSP