10min

New Anti-Cybercrime Law of Qatar 101

… for infosec geeks.

Sherif Eldeeb
http://eldeeb.net

First things first …

- I am not a lawyer.

- I did not write the law ☺.

- Few clauses in that law are considered controversial by many … we're not here today to sort those out (even though we'll have few of them mentioned…)

- The `official` name is "Law No. (**14**) of Year 2014 on Anti-Cybercrime".

The need for a "New" Law ...

- *Nulla poena sine lege*: (One cannot be punished for doing something that is not prohibited by law).

- The "old" one was (clauses 370:387) in the Common penalty law .

-Inefficient, inaccurate and led to many criminals "getting away with it".

“Ignorantia legis neminem excusat”

“ignorance of the law excuses no one”

Why should we care “as infosec folks”?

Governmental agencies, organizations, institutions, authorities, and companies affiliated with the government shall be committed to the following:

1- Undertake necessary preventive security measures to protect its Information Systems, electronic Websites, Information Networks, and Electronic Information and Data.
2- Report promptly, whenever detected, to the Competent Authority about any crime set forth in this Law, or any attempt to capture, intercept, or eavesdrop in an illegal manner; and provide the Competent Authority with all the necessary information to unveil the truth.
3- Retain Information Technology data and Subscriber Information for period of not less than (120) days, and provide the Competent Authority with such data.

Cooperate with the Competent Authority in exercising its competencies

Mandatory requirements

- Take “necessary preventive security measures” to protect information systems.
- Promptly reporting issues to `competent authority.`
- Keep logs for 120 days.
- Does NOT apply to private sector.
- Might eventually affect MSS

-(Gaining access/logging in) to any system (e.g. default/common password checking on .qa IP ranges, admin/admin for web, root/root for SSH …etc.).

-… penalty doubles if data was copied from those systems.

-… penalty doubles, yet again, if it turned out to be a .gov.qa or semi-.goc.qa system.

-Another example would be Aircrack'ing and connecting.

-**This includes unauthorized access of insiders (e.g. dishonest sysadmins, or malicious/nosy employees)**

-Penalty (3 years, 500,000QAR) max.

Bad stuff …

Gaining unauthorized access to information systems

Other bad stuff

-Impersonation (careful!)

-Extortion/sextortion

-MiTM, sniffing, intercepting … etc.

-Porn: spreading, selling, offering to others … etc. (simple `possession` is fine though)

-*Anything* related, even remotely, to child porn “including `simple` possession”.

- The `normal` bad stuff “e.g. aiding terrorists, carding, fraud, intellectual property,

-“…violating the social principles or values”

-“Publishing … (stuff) … connected to the sanctity of the personal or family life of *any* person, even if it is true”

-Operating a website that is used to spread false news (even though the law limited this to: ***with the aim to jeopardize the State safety, its public order, or its internal and external security)***

Controversial clauses

Concept: A law is considered `vague` only if an average citizen cannot generally determine what persons are regulated, what conduct is prohibited, or what punishment may be imposed…

Questions?

Thanks!