


2021年9月24日



The problems when Corporate deploying the Network Security law in integrated multi Information Security Compliance environment (Case Study) 企業在集成的多信息安全合規環境中部署網絡安全法時面臨的問題（案例研究）

By Ronald Pong

About Me 关于我:

- 姓名: 庞博文 (Ronald Pong)
- 专业: 信息安全专家 (支付卡安全, 电子取证和犯罪调查, 古典密码学, 信息安全法规及管理, 网络对抗, 信息安全监控中心)

- 职称: 首席执行官 (Nexusguard Consulting)
- 职称: 院长 (香港信息安全学院)
- 职称: 讲师 (香港品质保证局)
- 职称: 讲师 (香港大学专业进修学院)
- 职称: 创办人 (Dionysus Insurance Brokers)
- 职称: 创办人 (TOZ Captive Insurer)

- 香港政府资讯科技总监办公室 - 云端保安及私隐工作小组 增选成员 (WGCSP) (第二届)
- 香港政府资讯科技总监办公室 - 智慧灯柱技术咨询专责委员会 专家组成员
- 香港金融管理局 - 银行网络防卫计划(第一届) 专家组成员
- 香港智慧城市联盟 (Smart City Consortium) - 信息技术治理委员会 (Information Technology Governance Committee) 主席
- 香港公鑰基礎設施論壇 (Hong Kong Public Key Infrastructure (前主席) 現為副主席)

- 支付卡安全性评估员 Qualified Security Assessor (PCI QSA)
- 支付卡应用安全评估员 Payment Card Application Security Assessor (PA QSA)
- 中国信息安全测评中心注册信息安全培训讲师 (CISI)
- 香港注册信息安全专业人员 (CISP)
- 英国标准协会集团 ISO / IEC 27000:2013 信息安全管理体系审核员 / 主任审核员
- APMG-International IT 服务 (信息技术基础架构库) 管理体系审核员 Information Technology Services Management (ITIL)

企業在集成的多信息安全合規環境中部署網絡安全法時面臨的問題（案例研究）

What I did in last year at Macau? (我们去年在澳门发现了什么?)

- We are the Information Security Professional service company who provide service of InfoSec Compliance audit and consulting in Asia, in last year at the Macau Special Administrative Region of the People's Republic of China we did perform around seventy or up gap analysis projects for Macau Cybersecurity Law ("MCSL"). Our coverage included government department, critical infrastructure, financial institute, and entertainment Group. 我们是亚洲地区提供InfoSec合规审计和咨询服务的信息安全服务公司，去年在中华人民共和国澳门特别行政区，我们开展了大约70个澳门专业或以上的澳门网络安全法（“MCSL”）偏差分析项目。我们的覆盖范围包括政府部门、关键基础设施、金融机构和娱乐集团。
- We performed the gap analysis by designed questionnaire , online interview , face to face interview and technical network scanning. 我们通过设计问卷、在线访谈、面对面访谈和技术网络扫描进行了偏差分析。
- We take four and half months for finished our job. 我们用四个半月的时间完成我们的工作

企業在集成的多信息安全合規環境中部署網絡安全法時面臨的問題（案例研究）

The similarities of Hong Kong Special Administrative Region and Macau Special Administrative Region in the information security regulatory environment (香港特別行政區澳門特別行政區在信息安全法規環境當中的相同之處)

We can take Macau SAR as an example for forecast what will happen if Hong Kong SAR deploy the similar Cybersecurity Law. 我們可以以澳門特別行政區為例，預測如果香港特別行政區部署類似的《網絡安全法》會發生什麼。

Because: 因为：

- The Cybersecurity Law for SAR of China will inheritance some of the same factors from China Cybersecurity Law with no doubt. Specially in the method of classification model in data sensitive level, also in definition and requirement of data storage transborder law. 中国特区的网络安全法将无疑继承中国网络安全法的一些相同要素。特别是在数据敏感层面的分类模型方法，以及数据存储跨界法的定义和要求。
- In both Special Administrative Region they have a lot of companies are international company or transborder business around the world. They need to compile the law and regulation from around world included listed company requirement , industrial compliance , various privacy law and taxes or business regulation etc.. And all of those law, regulation and compliance have requirement in Information Security Management and Operation. 在这两个特别行政区，他们有很多公司是在世界各地开展业务的国际公司或跨国公司。他们需要遵守来自世界各地的法律和规定，包括上市公司要求、行业合规、各种隐私法和税收或商业法规等。所有这些法律、法规和合规对信息安全管理与运营都有要求。
- In both In both Special Administrative Region most of the company are both following the same or similar International Information technical management system included the formate of policy , procedure and management system. 在这两个特别行政区中，所有公司都遵循相同或相似的国际信息技术管理体系，包括政策、程序和管理体系的形式。
- In both In both Special Administrative Region most of the company using technical device, security safeguard device, technology are provided by english based Western vendor, included the support and management services provider. 在这两个特别行政区中，大部分公司使用的技术设备、安全保障设备、技术均由基于英语的西方供应商提供，包括支持和管理服务提供商。

So the difficulty in technical management layer special in infoSec management, what is happening in Macau SAR will happen in Hong Kong SAR. 所以技术管理层特别在infoSec管理上的困难，在澳门发生的事情，在香港特区也会发生。

Actually we seen the similar situation in some of our client in Hong Kong SAR already. We try to integrate the multi compliance and regulation requirements from different legal system for make it more cost effective and efficient. 事实上，我们已经在香港特别行政区的一些客户身上看到了类似的情况。我们尝试整合来自不同法律体系的多重合规和监管要求，使其更具成本效益和效率。

企業在集成的多信息安全合規環境中部署網絡安全法時面臨的問題（案例研究）

According to our experience in performing the audit and gap analysis in projects. We find the following issues: 根据我们在项目中进行审计和差距分析的经验。我们发现以下问题：

Terminology Gap 术语差距：

- They are using the different professional language in Information technology ! 我们在信息技术领域使用不同的专业语言！
- Most of the technical staff be trained to use English technical jargon for perform their work. 大多数技术人员都接受过使用英语技术术语的培训来进行工作.
- Example:
 - Password and Encryption or Cryptography (密碼/口令/加密)
 - In year 2019 When the Government of People's Republic of China published the China Encryption Law 《中国国家密码法》 . Almost of the Chinese Media included the Technical Magazines, New Paper , TV and KOL they all think China Government try to set up a law to collect and manage the password of citizen. 2019年中华人民共和国政府颁布了《中国国家密码法》。几乎所有的中文媒体包括技术杂志、新报、电视和KOL，他们都认为中国政府试图制定一项法律来收集和管理公民的密码.....
- More: logout (注销?/ 登出?) / Data Masking (数据屏蔽?/脫敏系統?) / Key Encryption Key (密鑰加密鑰?/密码加密码?)
 - We need to write a Terminology document for synchronise the technology jargon in English , Simplify Chinese and Traditional Chinese , also mapping with GB and ISO standard for basic, some time we also need to mapping with multi-compliance documents such as HKMA , SGMA, SOX 404, PCI DSS, GDPR , BASL etc..... or more 我们需要编写 Terminology 文档来同步英文、简体中文和繁体中文的技术术语，还需要对基本的 GB (国标) 和 ISO 标准进行映射，有时我们还需要与多合规文档映射整合如 HKMA、SGMA、SOX 404、PCI DSS、GDPR、BASL 等..... 或更多

企業在集成的多信息安全合規環境中部署網絡安全法時面臨的問題（案例研究）

According to our experience in performing the audit and gap analysis in projects. We find the following issues: 根据我们在项目中进行审计和差距分析的经验。我们发现以下问题：

Technology Gap: 技术差距:

- Classification Model of Risk 风险分类模型
 - In SAR when performing the infoSec impact analysis for security management, we use the Business impact as a major factor. But under the requirement of Cybersecurity law the infoSec impact analysis are rely on the 《网络安全等级保护制度》 (Network Security classification level system) the major factor is classify by national security impact. That means the organisation need to rebuild the Classification Model of Risk. 在特区进行安全管理的信息安全影响分析时，我们将业务影响作为主要因素。但在网络安全法的要求下，信息安全影响分析依赖于《网络安全等级保护制度》，主要因素按国家安全影响进行分类。这意味着组织需要重建风险分类模型。
- National Vulnerability DataBase 国家漏洞数据库
 - When we are performing the Security Vulnerability scanning and penetration testing we need to release on rely on the Vulnerability DataBase but there are no vulnerability DataBase can cover all the product on the world. If there are some product only resell in China, that mens only China National Vulnerability DataBase has recorded their known vulnerabilities. The same situation is existing in most of the countries. So we always suggest to never or control the percent of mixing cult-countries technical product. If not the vulnerability management will became complexation. That will also influence the the effectiveness of security monitoring and incident response. 我们在进行安全漏洞扫描和渗透测试时需要依赖漏洞数据库进行发布，但是没有漏洞数据库可以覆盖全球所有产品。如果有一些产品只在中国转售，那只有中国国家漏洞数据库记录了他们已知的漏洞。大多数国家都存在同样的情况。所以我们总是建议永远不要或控制混合多国技术产品的百分比。否则，漏洞管理将变得复杂。这也会影响安全监控和事件响应的有效性。

企業在集成的多信息安全合規環境中部署網絡安全法時面臨的問題（案例研究）

According to our experience in performing the audit and gap analysis in projects. We find the following issues: 根据我们在项目中进行审计和差距分析的经验。我们发现以下问题：

Legal Gap 法律差距

- Cryptographic algorithms and protocols 密码算法和协议
 - When we design how to compile the Cryptographic algorithms and protocols law for multi-countries at the same time, we found that is extremely complex 当我们设计如何同时遵守多国密码算法和协议法时，我们发现这是一个非常复杂的问题
- Transborder Data Flows and Data Privacy Law 跨境数据流和数据隐私法
 - We found there are difficulty to define the storage location and data flow load-balancing with system effectiveness. 我们发现在定义存储位置和数据流负载平衡与系统有效性方面存在困难。
 - We also found according to compile the requirement from multi-countries Transborder Data Flows and Data Privacy Law the data base will became more and more complex , specially in entreatment and service business. 我们还发现，根据多国跨境数据流和数据隐私法的要求，数据库将变得越来越复杂，特别是在娱乐和服务业务方面。

Human competency Gap

- Human competency and professional license 人的能力和专业执照
 - In both SAR the information security professional are holding the CISSP or other Western license for maintain their professional-ship. Only few people are holding the China CISP license , also the China CISP license are lecturing and exam by Simplify Chinese language. 在这两个特别行政区中，信息安全专业人员都持有 CISSP 证书或其他西方证书以保持其专业性。只有少数人持有中国CISP 证书，而且中国CISP 许可证是用简体中文授课和考试。

企業在集成的多信息安全合規環境中部署網絡安全法時面臨的問題（案例研究）

建議的解決方法

Vertical and Horizontal approach in deployment process 部署過程中的縱向和橫向方法

- From the experience of Macau SAR the government is using the Vertical approach in deployment process. That means they will let the government department deploy the Cybersecurity law at the first, secondly vertically deploy to various industrial segment layer by layer. That is a logical workable method but need time. 根據澳門特區的經驗，政府在部署過程中使用垂直方法。這意味着他們將首先讓政府部門部署網絡安全法，然後逐層垂直部署到不同的行業領域。這是一種合乎邏輯的可行方法，但需要時間。
- For Hong Kong SAR according to the number of business company and their size are more larger than Macau SAR. Vertically deploy may take a long time, more longer time will make the potential threat or problem will be unexpected. We suggest mixed the Vertical and Horizontal approach in deployment process at the same time. Horizontal approach is when deploying the Cyber security law in various industrial segment layer by layer also using make this as a requirement of their supporting service provide. The result will more like a ripple effect for making the deployment period can be compressed. 香港特別行政區商業公司的數量和規模比澳門特別行政區大。垂直部署可能需要很長時間，時間越長，潛在的威脅或問題就會出乎意料。我們建議在部署過程中同時混合使用垂直和水平方法。橫向方法是在各個行業部門逐層部署網絡安全法時，也將此作為其支持服務提供的要求。結果將更像是一個漣漪效應，使得部署周期可以被壓縮。

Educational approach

- Training of Expert in Technology - increase the number of CISP let them know the different in both Chinese and Western products, also learn how to integrate them together in same technical framework. 技術專家培訓——增加CISP的數量，讓他們了解中西產品的不同之處，並學習如何將它們整合到同一技術框架中。
- Training of Expert in Security Management - increase the number of expert in Security Management system special focus on compliance and regulation of both Chinese and Western requirement from different legal framework 安全管理專家培訓 - 增加安全管理系統專家的數量，特別關注來自不同法律框架的中西方要求的合規性和監管。

Grace period 寬限期

- Grace period is extremely important for all the organisation when deploying the Cybersecurity law. According to the requirement of staff training, production selection and replacement, redesign the Classification model of Risk and Risk calculation. 在部署網絡安全法時，寬限期對所有組織都極為重要。根據員工培訓、產品選擇和補充的要求，重新設計了風險和風險計算的分類模型。
- We suggest the first phase of grace period need to be at least 3 to 4 years. 我們建議第一階段的寬限期至少需要3到4年。