PSU

PIPL, challenge and opportunity!

Lars-Åke Severin

CEO & Founder PSU

御安行创始人兼总裁林奇辉先生

- Lars-Åke Severin is the founder and CEO of the Security Consultancy firm PSU. Lars-Åke has a background from the Swedish Armed Forces, the Swedish Police and Swedish Security Police (SÄPO). Lars-Åke operationally led the Swedish Royal Family Close Protection Teams and founded Her Royal Highness Crown Princess Victoria's Close Protection Team.

  林奇辉先生是具有斯堪的纳维亚背景的领先的安全咨询公司--北京御安行安全防范技术咨询有限公司的创始人和首席执行官，曾任职于瑞典武装部队、瑞典警队和安全警察部队。他曾领导过瑞典王室护卫队，创建了维多利亚王储殿下的护卫队.

- Lars-Åke founded PSU in China in 2006 and is one of the leading foreign experts on security management in China. Lars-Åke is also Director and member of the board of the Swedish industrial company Bulten (China). From 2010 to 2016 Lars-Åke served as Director of the main board for Swedish Chamber of Commerce in China and from 2016-2021 as its Chairman.

  林奇辉先生于 2006 年在中国成立了御安行，是中国领先的外国安全管理专家之一。 他还是瑞典布尔顿紧固件（中国）有限公司的董事及董事会成员。 林奇辉先生于2010 年至 2016 年担任了中国瑞典商会董事，于 2016 年至 2021 年担任其主席.

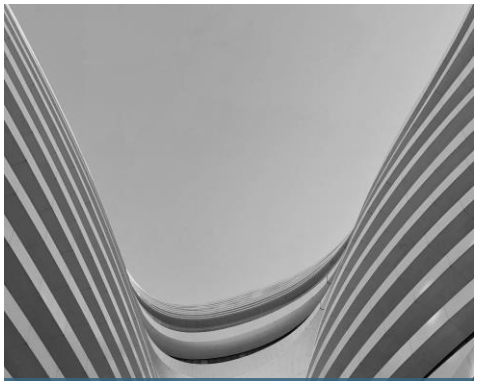
- Lars-Ake is an often engaged speaker on Risk Management Strategies in complex environments.

  林奇辉先生经常获邀就复杂环境下风险管理策略发表演讲.

larsake@psuchina.com +8618611521166

Who we are

Established in 2006 and is one of the leading Risk & Security Consultancies in China



We deal with security related issues connected to

- Corporate
- Brands
- Individuals

We work throughout strategic partnership in Asia, Europe and the US.

Our Services

Preventive

Investigative

Protective

GDPR was developed at least in part as a people's and states reaction to surveillance operated by the U.S. and UK intelligence agencies and revealed by Edward Snowden. It is primarily aimed at protecting European citizens and residents. PIPL, however, is also closely aligned with China's international intent to dominate emerging technologies and especially those that rely on data usage.

PIPL, Personal Information Privacy Law (2021)

“It's a major piece of legislation and regulation which should be seen as a part of the series of regulatory moves by the government of China to protect personal information but also to rebalance the power that exists between big tech specifically, and the Chinese government,”

PSU 御安行

China reportedly warns local tech companies of increased cybersecurity oversight

In China, rules for companies listing overseas will be revised and publicly-traded firms will receive greater scrutiny regarding how they handle data, according to Bloomberg.

China has reportedly warned local companies it will tighten oversight of data security and overseas listings days after unveiling Didi has been subject to a government cybersecurity review.

BEIJING, July 27 (Reuters) - Tencent's (0700.HK) WeChat has temporarily suspended registration of new users in mainland China as it undergoes a technical upgrade "to align with relevant laws and regulations", China's dominant instant messaging platform said on Tuesday.

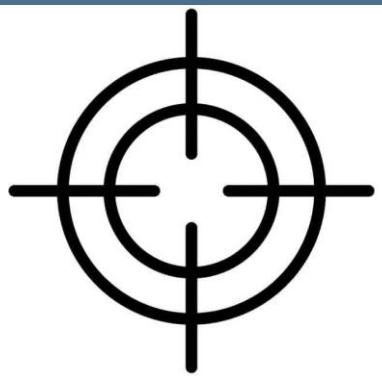
"We are currently upgrading our security technology to align with all relevant laws and regulations," the company said in a statement to Reuters.

"During this time, registration of new Weixin personal and official accounts has been temporarily suspended. Registration services will be restored after the upgrade is complete, which is expected in early August," it added.

Weixin is the Chinese name for WeChat.

Shares in Tencent plunged 9.0% in Hong Kong on Tuesday amid widespread market jitters over Chinese regulatory crackdowns on high-growth sectors, benchmark Hang Seng Index (HSI) fell 4.2%.

High tech might find themselves in the cross hair but all businesses must arrange full focus



China announces on-site cybersecurity investigati

China's cyber-watchdog has announced an on-site ride-hailing service Didi, stepping up scrutiny after of customer information caused the company's New

By **The Associated Press**

16 July 2021, 18:08 • 1 min read

Cyber Security Law (2017)

This is designed to regulate the network and platform providers, and how they handle personal data.

PIPL, Personal Information Privacy Law (2021)

Data Security Law (2021)

Looks at the protection of data more from the government's perspective. Stricter regulation of 'national core data'. Extraterritorial reach for data processing outside of China that might affect 'the national security, public interests, or lawful rights and interests of citizens and organizations in China'.

The three laws provide perhaps the strictest cybersecurity regulation found anywhere in the world and is a part of a global trend.

Cyber crime is a growing concern, much based on the fact that we all put a lot of private (and corporate information) online (global cyber crime + 600% during Covid -19).

“It would be wrong to assume that just because this is China, the result will be draconian. In some parts PIPL is less severe than western examples. For example, there is no imposed ‘adequacy’ framework such as that required by the GDPR. Adequacy frameworks can lead to problems – such as a current EU ruling threatening data flows between the EU and the U.S. China demonstrates perhaps an understanding of the importance of international trade.

It is rarely smart to make a diagnosis of your own symptoms!

Basic IT environment
IT (security) policy and actual implementation and control/ follow up
Laptop usage, hard drive encryptions

Internal threats are more common than external
Lack of knowledge more common than malice, “unintentional breach”.

Mobile devices dominate desktop usage
During singles day, over 80% of sales were on mobile devices
+ 30 % of mobile internet time is spent on WeChat
Well over 70 % of China population are active internet users

How many have a corporate phone? A smartphone is not a phone, it’s a computer

To judge someone for the future, you need to know about their past!

PIPL, provides a risk of even less background & compliance researches
which creates a risk exposure

PSU 御安行

Consent is they key word!

Define in contractual agreements usage of any private information.
Ask not only for consent but also provide information how to withdraw consent!

Act as transparently and informatively as possible and by that, mitigate future complaint.
“Walk the extra mile”

Where are you right now?

Situational awareness!

PIPL check list, implementation, awareness training and red flag audit (control compliance).

Processes must be designed and defined in terms of data collection and consent must be secured before processing any private personal information. Information must be given that provide clarity on erasing private identifiable information after finalisation or, in the consent, acceptance for storage of such information.
Avoid future conflicts!

The PIPL uses the term “personal information processing entity” to refer to “organization or individual that *independently determines the purposes and means for processing of personal information”*

Third parties must be clearly professional and describe, when provided private data, that it will be used only for the assigned purpose.
Third parties need to provide you with a information security clause that shows that the actual usage is only in accordance with agreed scope.
Storage time and secured destruction of provided information must be described (or “anonymised)”

PSU
御安行

Q&A

Contact info

Beijing

Room 1601, Building A

Tower 2, WangJing SOHO

No.1 FuTong East Street

ChaoYang District

Beijing P.R China

Office: +86 10 6471 9619

info@psuchina.com

www.psuchina.com.cn

Shanghai

Room 710, Building B

Far East International Plaza

No.317 Xianxia Road

Changning District

200051 Shanghai

Office: +86 21 52125970

Fax: +86 21 52125972