

October 5, 2018

## Chinese Cybersecurity Law







Edward McNicholas  
Sidley Austin LLP

Hugo Teufel  
Raytheon

SIDLEY AUSTIN LLP  
**SIDLEY**

**Raytheon**

# The Threat Actors

	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS						
MOTIVATION	Hacktivists use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Trusted insiders steal proprietary information for personal, financial, and ideological reasons.	Nation-state actors conduct computer intrusions to steal sensitive state secrets and propriety information from private companies.	Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.	Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

# Cybersecurity Involves More Than PII

---

***Valuable IP assets, proprietary information***, business, transaction and negotiating records, financial data, electronic funds, business functionality and continuity

***Proprietary Research and Techniques***

industrial control systems (ICS): computer systems that monitor and control industrial, infrastructure, or facility-based processes

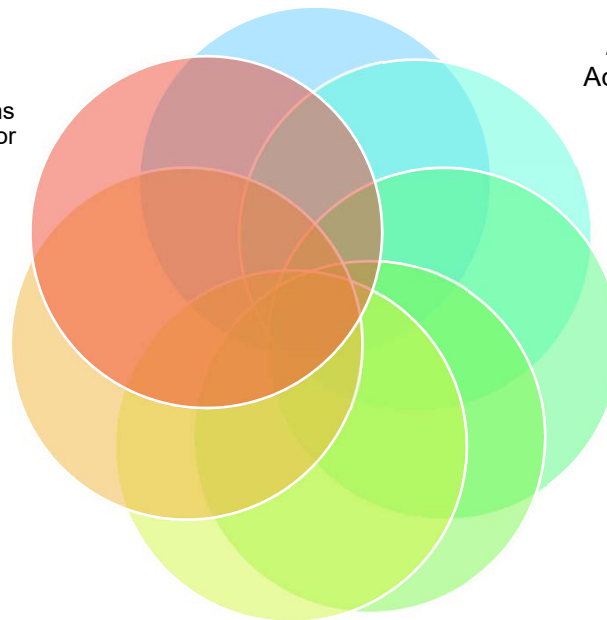
***Personal information;***  
Account information; access to accounts

***Supply chain management***

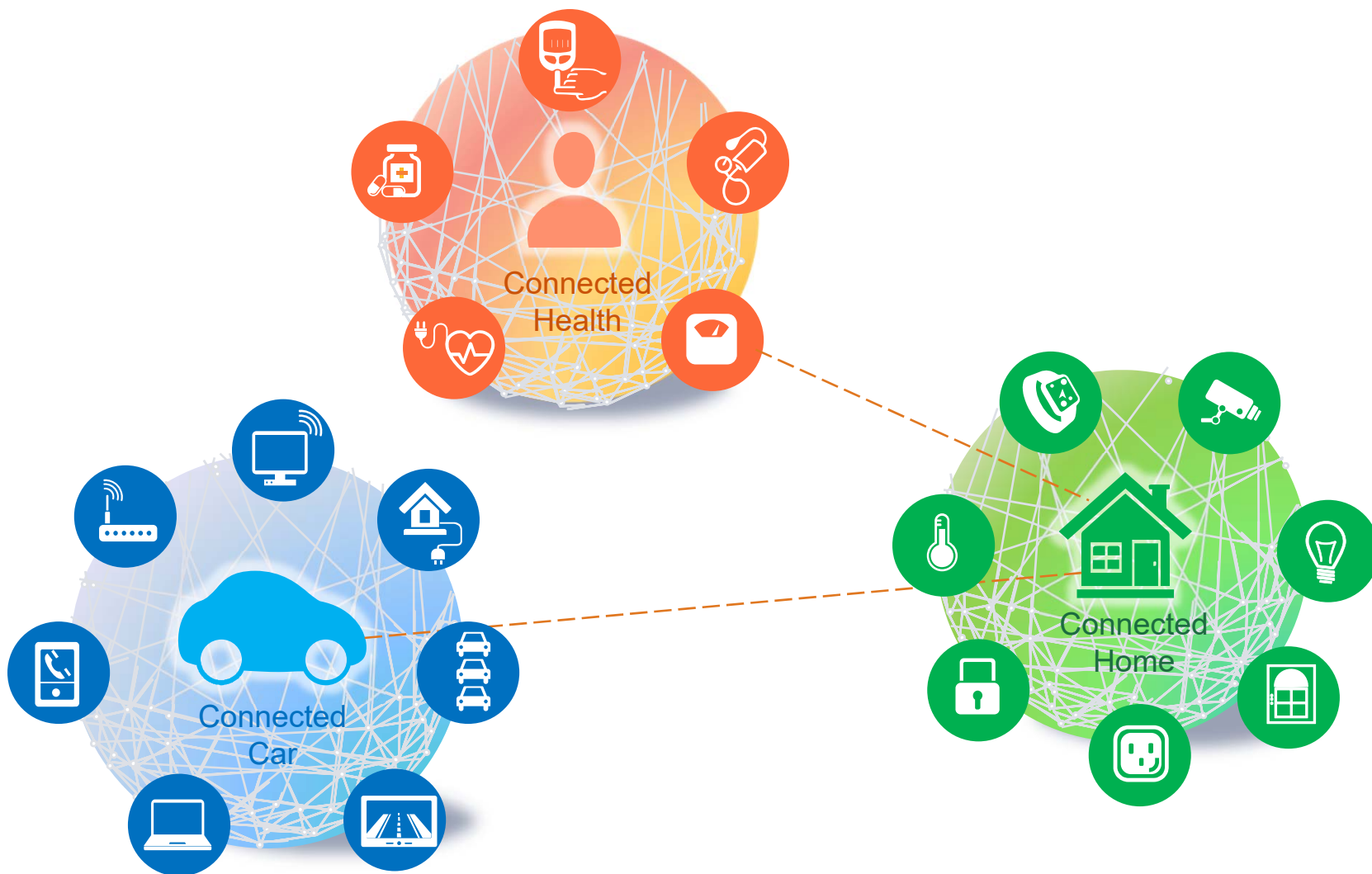
***Disruption of business;***  
denial of service; cyber-extortion

***Communication systems***

***Critical infrastructure***  
and essential services



# Connections – And Attack Vectors – Are Growing Exponentially



***“without cybersecurity there  
is no national security”***

President Xi

## China's Ministry of Foreign Affairs

**China is a resolute defender of cybersecurity.** It advocates for the international community to work together on tackling cybersecurity threats through dialogue on the basis of mutual respect, equality and mutual benefit.

Supply chain safety in cyberspace is an issue of common concern, and **China is also a victim.** China, Russia, and other member states of the Shanghai Cooperation Organization proposed an “International code of conduct for information security” to the United Nations as early as 2011. It included a pledge to ensure the supply chain security of information and communications technology products and services, in order to prevent other states from using their advantages in resources and technologies to undermine the interest of other countries. We hope parties make less gratuitous accusations and suspicions but conduct more constructive talk and collaboration so that we can work together in building a peaceful, safe, open, cooperative and orderly cyberspace.

—Translated by Bloomberg News in Beijing

<https://www.bloomberg.com/news/articles/2018-10-04/the-big-hack-amazon-apple-supermicro-and-beijing-respond>



***“Thousands”*** of  
U.S. companies have  
been cyber-attacked  
by the Chinese  
government.

-- John Carlin, former National Security Division,  
U.S. Department of Justice,  
60 Minutes, Jan. 17, 2016.



# China's Cybersecurity Law

---

- Law came into force on June 1, 2017.
- As early as July 1, 2015, the *National Security Law of the People's Republic of China* was promulgated, expressly provided that the state shall “safeguard **sovereignty** and security of cyberspace in the state” -- a key theme.
- The Chinese Cyber Security Law strengthens the protection and security of key information infrastructure and Important Data
- Article 21 requires **network operators** to back up and encrypt Important Data
  - Imposes certain obligations on the “network operators,” which is defined to include owners and administrators of networks, and network service providers
- Article 37 requires operators of “key **information infrastructures**” to be subject to data localization for personal data and Important Data they collect within China



## Not the American Vision of a Free Internet

---

**Article 12:** The State protects the rights of citizens, legal persons, and other organizations to use networks in accordance with the law; it promotes widespread network access, raises the level of network services, provides secure and convenient network services to society, and guarantees the lawful, **orderly**, and free circulation of network information.

Any person and organization using networks shall abide by the Constitution and laws, **observe public order, and respect social morality**; they must not endanger cybersecurity, and must not use the Internet to engage in activities endangering national security, **national honor, and national interests**; they must not incite subversion of national sovereignty, overturn the socialist system, incite separatism, **break national unity**, advocate terrorism or extremism, advocate ethnic hatred and ethnic discrimination, **disseminate violent, obscene, or sexual information, create or disseminate false information to disrupt the economic or social order, or information that infringes on the reputation, privacy, intellectual property or other lawful rights and interests of others, and other such acts.**

## Also a Data Protection Law

---

- The cybersecurity law includes provisions for the protection of personal information, such as
  - Users must be informed about and consent to the collection and uses of data (Article 22)
  - Personal information must be maintained in a legal manner (to be specified by regulations) consistent with principles of legality, propriety, and necessity (Article 41)
    - Purposes must be explicitly stated
    - Gathered information must be related to the services provided
  - Security measures required as well as data breach notice to users and regulators (Article 42)
  - Users can request corrections of errors; deletion if the network operator violates the law (Article 43)
  - Theft of personal information is illegal (Article 44)
  - Personal information must be kept confidential (Article 45)

## Critical Information Infrastructure Operators

---

- “Critical information infrastructure” for “public communication and information services, power, traffic, water resources, finance, public service, e-government, and other **critical information infrastructure** which—if destroyed, suffering a loss of function, or experiencing leakage of data—might seriously endanger national security, **national welfare, the people’s livelihood, or the public interest.**” (Article 31)
- **Enhanced obligations (Article 34)**
  - specialized security management bodies and persons responsible for security management, and conduct security background checks on those responsible persons and personnel in critical positions
  - Periodically conduct cybersecurity education, technical training, and skills evaluations for employees
  - Conduct disaster recovery backups of important systems and databases;
- “Critical information infrastructure operators purchasing network products and services that might impact national security shall undergo **a national security review** organized by the State cybersecurity and informatization departments and relevant departments of the State Council.” (Article 35)

## Localization

---

- Under Article 37 of China's Cybersecurity Law (already effective from Jun. 1, 2017), Critical Information Infrastructure Operators ("CIIOs") are still subject to data localization requirements.
- A more wide-ranging data localization requirement was removed from the draft regulation as pertaining to "network operators," but it may be added back into the law
- The localization requirements would make the contents of data subject to access by Chinese law enforcement and intelligence services under Chinese law

## Network Operators

---

- “network” includes networks and systems that are composed of computers and other information terminals and the relevant facilities and used for purposes of collecting, storing, transmitting, exchanging and processing information in accordance with certain rules and procedures. (Article 73).
- Requirements include:
  - compliance with a series of requirements of tiered cyber protection systems (Article 21), such as:
    - technical measures to prevent computer viruses, cyber attacks, network intrusions, and other actions endangering cybersecurity;
    - technical measures for monitoring and recording network operational statuses and cybersecurity incidents, and follow provisions to store network logs **for at least six months**;
    - measures such as data classification, backup of important data, and encryption;
  - verification of users’ **real identity** (for certain network operators) (Article 24);
  - formulation of cyber security emergency response plans (Article 25); and
  - assistance and support necessary to investigative authorities where necessary for protecting national security and investigating crimes (Article 28).

# Personal Information Security Specification

- Formulated by the National Information Security Standardization Technical Committee, a standards-setting body known as TC260, which operates under the Cyberspace Administrations, China's Internet regulator
- Standards are recommended rather than mandatory, but enforcement shows that they are essentially required.

Standards are planned for:

- security guidelines for cloud computing
- security capability requirements; and
- assessing security capabilities.



## China's VPN Rules

---

- As of March 31, 2018, businesses can use only VPNs approved by the Chinese government.
- Before the change:
  - many people used unauthorized VPNs to access websites blocked in China
  - the VPN rules were very vague and essentially not enforced.
- Now there is a concerted effort to ban “everything that is not approved, registered, or reviewed by the government.”
- It is costly, but possible, to switch from a VPN to a dedicated line that provides direct connection between their Chinese subsidiary and headquarters
- The other real option is to use a sanctioned VPN provided by China Telecom.



# China's Cross-Border Data Transfer Regime

---

- On May 27, 2017, China's National Information Security Standardization Technical Committee, a standard-setting committee jointly supervised by the Standardization Administration of China and the Cyberspace Administration of China ("CAC"), released the draft *Information Security Technology – Guidelines for Cross-Border Data Transfer Security Assessment* (the "Guidelines").
- On August 31, 2017, revised Guidelines issued.
- The Guidelines are national standards, not binding laws or regulations, but it can be anticipated that they will be closely followed by the relevant regulatory authorities in regulating the cross-border data transfer.
- Substantively, they require that a cross-border data transfer (even a one-time transfer) be lawful, legitimate, and necessary. Factors to include:
  - consent has been obtained from the individuals whose personal information is to be exported,
  - the data export complies with provisions under relevant treaties executed between the Chinese government and other countries or regions,
  - the data export is necessary for performing the ordinary business activities or the contractual obligations of the network operators, etc.

# China's New Cross Border Regime

---

- Two key implementing documents:
  - Regulation (i.e., the *Measures on Security Assessment of Cross-border Data Transfer of Personal Information and Critical Data*) (April 2017)
  - National standard (publicized in May 2017, revised August 31, 2017)
- Requires:
  - a network operator in China must obtain prior consent of the subjects for cross-border transfer of personal information, including the purpose, scope, recipients and country of destination
  - the network operator should conduct security assessment for cross-border transfer of data, which covers personal information
  - a network operator must retain assessment and report results if they meet thresholds set by the CAC or sector-specific regulator
- Unless the security assessment reveals major risks, companies may transfer Chinese citizens' personal information and "important data" outside of China
- Companies are incurring costs to review data and network assets and hire senior staff to manage cybersecurity risks

# China's Cross-Border Assessment Requirements

---

- Pursuant to the Guidelines, the process of security assessment includes following steps: (1) initiating self-assessments, (2) formulating data export plans, (3) assessing the lawfulness, appropriateness and risk controllability of the data export plans, (4) generating assessment reports, and (5) revising the data export plan and security measures.
- Network operators must assess whether the data export plan is lawful, appropriate and risk controllable by referring to the assessment methods set out in Appendix B of the Guidelines which outlines certain risk factors and their risk levels.
- Personal Information and “**Important Data**” shall not be provided overseas if the result of the security assessment shows a risk level of “high” or “extremely high.”
- The assessment report shall be retained for at least five years.

## What is “Important Data”?

---

- **“Important Data”** is data that could have “severe consequences” for national security or societal and public interests in the event of leak or misuse after being transferred outside of China.
  - Appendix A of the Guidelines lists important data and their identifying features in 28 industries and sectors. The definition, scope or identifying criteria for important data in these key industries may be further specified by the competent industry regulators.
- The National Information Security Standardization Technical Committee, a standards-setting body known as TC260 that operates under the auspices of the Cyberspace Administration, China’s Internet regulator, has started drafting a new set of standards for identifying important data.
- Important data is defined in general as data that is closely connected with national security, economic development and the public interest in the Measures for Conducting Security Reviews for Cross-Border Transfers of Personal Information and Important Data.

## Potential Effects of Cross-Border Transfer Regime

---

The net effect is that cross-border data transfers can be prohibited in any of the following circumstances:

- If the transfer does not comply with laws or regulations;
- Data subjects do not consent to the transfer of personal information;
- The transfer poses risks to China's national security or public interests;
- The transfer has the potential of endangering China's security of "national politics, territory, military, economy, culture, society, technology, information, ecological environment, resources, nuclear facilities and so on;" or
- Other circumstances in which the Chinese government determines that the data concerned is prohibited from being transferred offshore.

E.g., Apple Inc. has said it is spending \$1 billion to build a data center in Guizhou to comply with rules that cloud data from Chinese consumers be stored in China.

### Timing

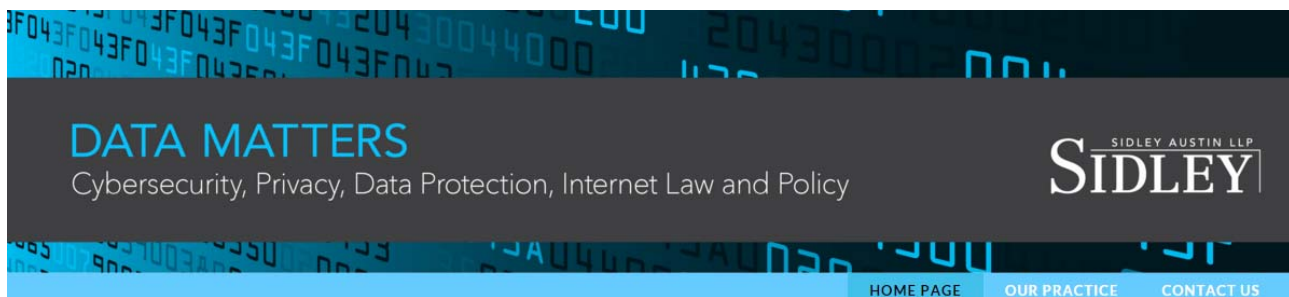
The Measures took effect on June 1, 2017, the same effective date as for the Law. They provide a grace period of 18 months for companies to comply with the rules and enforcement will start after December 31, 2018.


# The Catalog

---

- “Critical network equipment and specialized cybersecurity products shall follow national standards and mandatory requirements, and be **security certified by a qualified establishment or meet the requirements of a security inspection, before being sold or provided**. The state cybersecurity and informatization departments, together with the relevant departments of the State Council, will formulate and release **a catalog of critical network equipment and specialized cybersecurity products**, and promote reciprocal recognition of security certifications and security inspection results to avoid duplicative certifications and inspections.” (Article 23)
- On June 9, 2017, the Cyberspace Administration of China, the Ministry of Industry and Information Technology of the PRC, the Ministry of Public Security of the PRC along with the Certification and Accreditation Administration of the PRC jointly released the Catalog of Critical Network Equipment and Specialized Cyber Security Products (Batch I) (“Catalog”), which became effective on June 1, 2017.
- The Catalog supplements the security certification or security detection requirement for the critical network equipment and specialized cyber security products under Article 23 and outlines the types of equipment and products with specification parameters.

# Sidley's Data Matters Blog



Type keywords... 

## CONTACTS



## Patient Access and Medicare Protection Act

 JAN 07 2016  ANNA SPENCER AND RINA MADY

On December 28, 2015, President Obama signed into law S. 2425, the Patient Access and Medicare Protection Act (the "Act"). In addition to provisions intended to ensure that Medicare reimbursement policies promote continued access to certain durable medical equipment, like wheelchair accessories, the Act includes provisions that affect adoption of Health Information Technology ("HIT") and those that provide greater protection against medical identity theft. Specifically, the Act recognizes various categories of hardship exceptions from meaningful use requirements for the 2015 reporting period and strengthens the penalties associated with medical identity theft.

[\(MORE...\)](#)


SHARE



 [COMPUTER CRIMES, CYBERSECURITY, ENFORCEMENT, HEALTH PRIVACY, IDENTITY THEFT](#)

## OFAC issues Cyber-Related Sanctions Regulations

## CATEGORIES

Select Category 

## UPCOMING EVENTS

[2016 Derivatives and Futures Law Committee Meeting](#)

January 21 - January 23

[Data Protection in Finance 2016](#)

January 28

[SIFMA 2016 Compliance and Legal Society Annual Seminar](#)

March 13 - March 16

<http://datamatters.sidley.com/>