RISK
RESILIENCE
REPUTATION

Strategies to Navigate the Evolving Cyber & Data Landscape in China

达沃
DA WO
LAW FIRM
SHANGHAI

in partnership with

Teneo®

达沃
DA WO
LAW FIRM
SHANGHAI

Updates to China's Cybersecurity and Data Protection Framework

Who is DaWo?

A TRULY LOCAL-INTERNATIONAL BOUTIQUE LAW FIRM IN SHANGHAI

DaWo is a registered and fully licensed PRC law firm with a global background. Based in Shanghai, our clients hail from all over the world, and they rely on our internationally-trained lawyers and associates for expert, effective legal assistance in China. We are big enough to make a real difference for your business, but small enough that you know we really care.

INTRODUCTION

This presentation will cover cybersecurity compliance and data protection in China, including recent and upcoming updates to China's cybersecurity and data protection framework, a few enforcement actions, and what to do in the event of a data breach.

OVERVIEW

A PATCHWORK OF REGULATIONS

China's data protection framework is pieced together from various rules contained in a number of different laws, measures and regulations.

The key texts:

- Cybersecurity Law
- Personal Information Security Specification
- Personal Information Protection Law
- Data Security Law

Personal Information Security Specification

Personal Information Protection Law

Guidance notices

Cybersecurity Law

- Effective from 1 June 2017
- First national framework for comprehensive regulation of electronically stored data

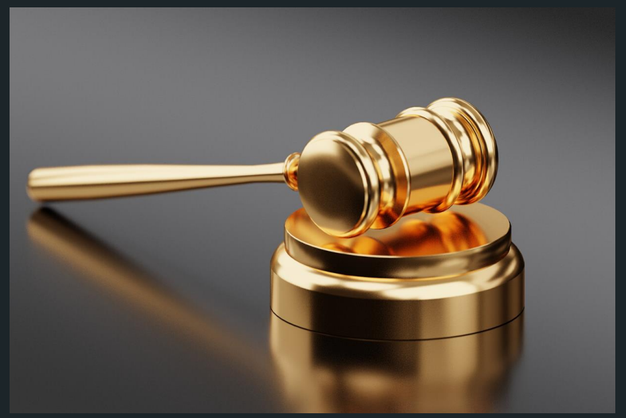
MPLS 2.0

Data Security Law

Technical Standards

Regulations

Strengthening the Framework



China, like other countries, views data as a nationally strategic resource. As such, it has been aggressive in creating a national cyber/data protection framework

Formulating a comprehensive law related to this has been on the NPC’s legislative agenda since September 2018, but it has not yet settled on draft language. We expect it will soon.

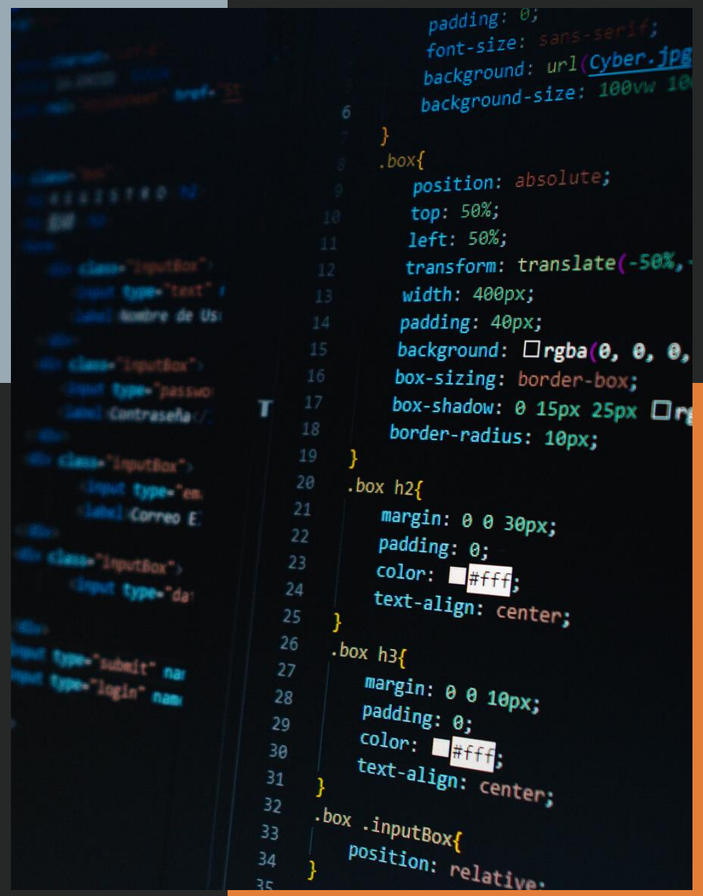
UPDATES

Known additions to China’s cybersecurity framework

Personal Information Security Specification (“2020 PIS”)/ Personal Information protection Law (“PIPL”)/Civil Code

Data Security Law

MLPS 2.0



New Version of the Personal Information Security Specification

2020 PIS - UPDATE

- Issued on 6 March 2020.
- The 2020 PIS effective 1 October 2020
- Highlights
  - Consolidates definitions and increases scope of protected personal information
  - Defines ‘consent’ – specific, informed, freely given, by affirmative action or passive act
  - Expanded obligations on third-party processors
  - Expanded requirements for data breach notification
  - Enhanced biometric protection
  - ‘protection/privacy by design’

PERSONAL INFORMATION PROTECTION LAW

Currently only a draft (not yet implemented)

On October 21, 2020, the Standing Committee of the National People's Congress (NPC) published a Draft Personal Information Protection Law (Draft PIPL) for public comment through November 19, 2020

8 chapters, containing 70 articles

Personal Information Handling Rules, Rules for Handling Sensitive Personal Information, Specific Provisions on Government Handling Personal Information, Rules on Cross-Border PI Transfer, Individuals' Rights, Personal Information Handlers' Duties, Oversight Authorities, Legal Liabilities

MAIN POINTS

- Focused on personal information protection
- Controversial extra-territorial application
- Privacy/personal information impact assessments
- Cross-border data transfer requirements clarified
- Data processing requirements/limitations clarified
- Interesting theoretical limitations of government's actions
- Major increases in penalties for violations

CIVIL CODE

approved on May 28, 2020

will take effect January 1, 2021

Right to Privacy

For the first time, stipulates that the right to privacy is part of recognized “personality rights.” Lays out legal bases for protecting privacy.

Personal Information

Sets out guidelines for processing of personal information (collecting, storing, using, transmitting, providing, and publicizing) people’s personal information. Extends protection to an even wider array of personal information than recognized before. Founded on considerations legality, necessity, and limitation in scope.

Tort Liability

Because privacy/personal information protection is now considered an inherent personality right, and the civil code provides for tort liability for violations of civil rights, it follows that infringements on privacy and personal data will carry tort liability.

DATA SECURITY LAW

Currently only a draft (not yet implemented)

On July 3, 2020, the Standing Committee of the National People's Congress (NPC) published a Draft Data Security Law (Draft DSL) for public comment through August 16, 2020

51 articles across 7 chapters

General Principles, Data Security and Development, Data Security System, Data Security Protection Obligations, Security and Opening of Government Affairs Data, Legal Liability and Miscellaneous

MAIN POINTS

- Focused on national security
- Controversial extra-territorial application
- Tiered classification system
- Data not covered by the draft DSL:
  - Military data, personal information, and state secrets will be covered by separate regulations.
- Security assessments
- Data protection obligations

MLPS 2.0

What is the MLPS?

- Article 21 of the CSL states that “the State has implemented a cybersecurity multi-level protection scheme. Network operators must perform … security protection duties … to ensure the network is free from interference, damage, or unauthorized access, and to prevent network data leaks, theft, or falsification…”
- The MPLS is a graded system of evaluating what security protection duties one has to perform.

MLPS 2.0

- A more robust series of standards/practices/supervision, extended beyond traditional network systems
- Emphasis on security capabilities, including threat prevention, detection, response

MLPS 2.0 FOCUS ON STANDARDS/LEVELS

IDENTIFY WHAT NEEDS TO BE GRADED, APPROXIMATE SECURITY LEVELS, AND APPOINT RESPONSIBLE PERSONNEL

PERFORM ASSESSMENTS (SELF /3RD PARTY) AND FORMULATE SECURITY MEASURES (POLICY, TECHNICAL, RESPONSIVE)

IMPLEMENT SECURITY MEASURES (POLICY, TECHNICAL, RESPONSIVE)

HOW TO APPROACH MLPS 2.0

RELEVANT CONSIDERATIONS

INTERNAL REVIEW

EXTERNAL REVIEW

FILING FOR APPROVAL/CERTIFICATION

WHAT SECTOR ARE YOU IN? IS IT HIGH-RISK?

WHAT KIND OF DATA DO YOU COLLECT/PROCESS? PERSONAL DATA?

IMPORTANT DATA? HOW MUCH?

IS THERE CROSS-BORDER TRANSFER?

CYBERSECURITY PLAYBOOK

WHAT DOES THE LAW SAY? BE PROACTIVE.

POLICY MEASURES

- Internal rules and structures

TECHNICAL MEASURES

- Internal network technology rules, standards, practices

RESPONSIVE MEASURES

- Internal contingency plans

FORMULATE YOUR STRATEGY

POLICY MEASURES

SELF-ASSESSMENTS

- At least reasonable precision
- Forms basis of compliance strategy

DRAFT INTERNAL POLICIES

- Comprehensive guidelines
- Certain roles must be designated

DRAFT RESPONSE POLICIES

- Contingency plans
- Immediately available/actionable

TECHNICAL MEASURES

TECHNICAL COUNTERMEASURES

- ANTI-VIRUS SOFT/HARDWARE
- ANTI-INTRUSION HARDWARE

MONITORING AND TESTING

- COMPREHENSIVE LOGGING
- PROACTIVE MONITORING
- ADDRESS ANOMALIES

BACKUP, RECOVERY, ENCRYPTION

- DO THIS REGULARLY

DATA INCIDENT PLAYBOOK

RESPONSIVE MEASURES IF SOMETHING GOES WRONG

NOTIFY AND INVESTIGATE

- ALL AFFECTED PARTIES
- ROOT-CAUSE INVESTIGATION

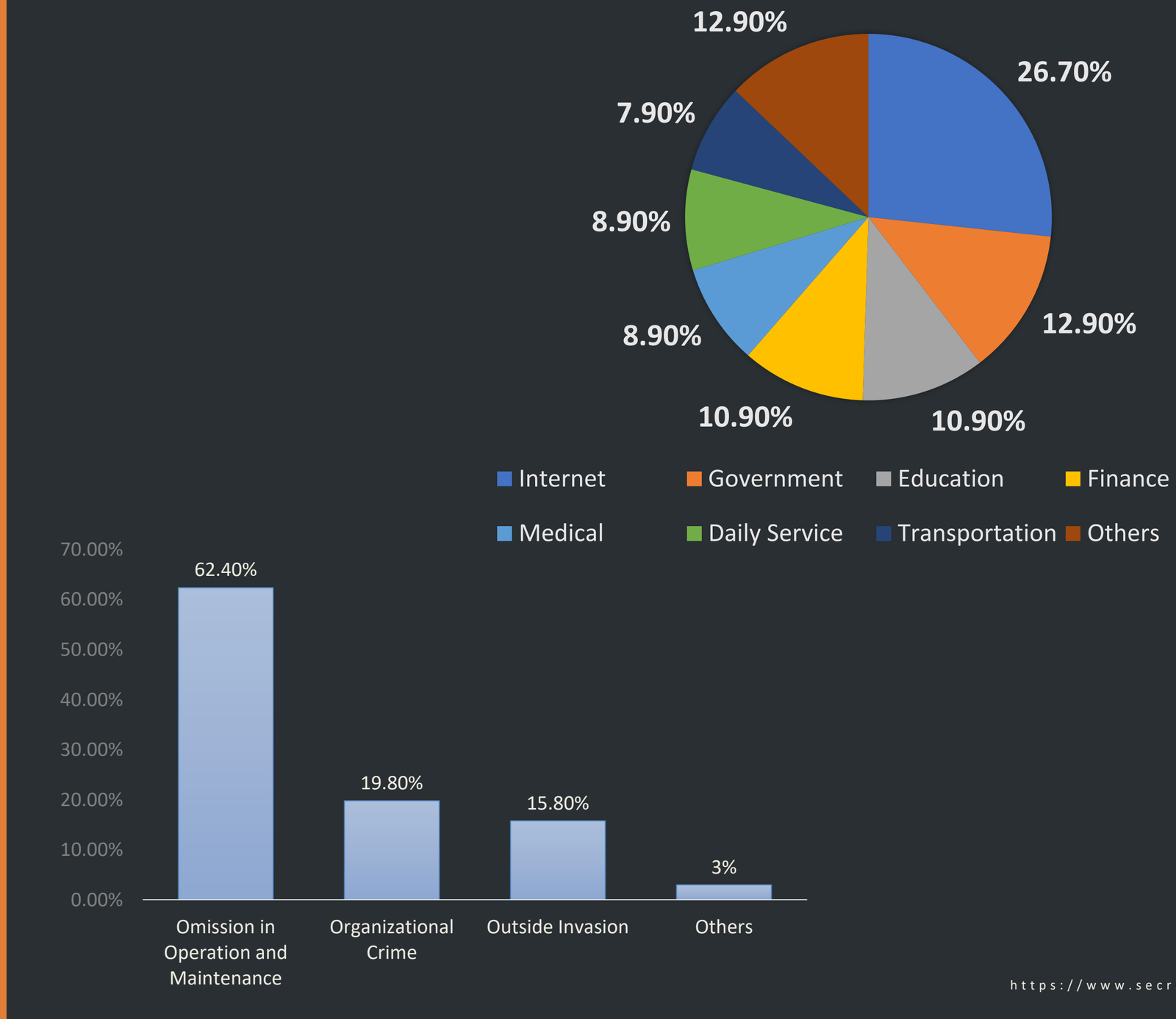
COLLECT AND COMMUNICATE

- RETAIN EVIDENCE (LOGS, MEMORY IMAGES, ETC.)
- OPEN COMMUNICATION WITH AUTHORITIES

LEARN

- COMPREHENSIVE REVIEW OF INCIDENT
- DISCUSS OPENLY HOW TO IMPROVE PROCESSES

ENFORCEMENT ACTIONS 2019-2020



CASE STUDIES

Failure to Notify Cyber Breach

A company's website was breached by a virus, leading to a relatively minor release of sensitive personal information. The responsible person at the company failed to promptly notify users and the authorities. A fine of 10,000 yuan was imposed on the responsible person individually.

Unreasonable Collection of Personal Information

An internet company collected user information, including accessing text messages, phone calls, etc. The PSB was notified and found the company had stored about 2.5 million pieces of user information. Six primary responsible people prosecuted and detained.

Failure to Protect Personal Information at Scale

In 2020, an internet company experienced a breach exposing 500 million users' personal information. It was required to:

- immediately overhaul its internal privacy policies;
- immediately overhaul incident reporting policies;
- immediately overhaul internal data security, risk management, compliance auditing.

Failure to Establish Internal Cyber Security Policy

In 2019, a securities investment consulting company's system was accessed illegally by the outsider and more than 10,000 pieces of personal information were stolen and leaked. The police has found that this company has failed to establish a Cyber Security Policy, The police then gives the company an official warning for such failure.

TO SUM UP

China has moved from having virtually no real national cybersecurity initiative less than five years ago, towards becoming one of the most tightly regulated cyber and data landscapes in the world.

China remains intent upon shoring up its cybersecurity framework, as seen through the constantly expanding, more and more comprehensive body of law. There are various reasons for this, including national security, desire for innovation, and of course control of data.

Even though large parts of the framework are not yet fully effective, we still recommend that businesses take a proactive approach in addressing the requirements found therein. To put it simply, China's Cybersecurity/Data Compliance framework is not going away, and it will only become more impactful as time goes on.

We offer training and other assistance with getting compliant under this evolving framework.

Nathaniel Rushforth

- Lawyer at DaWo Law Firm Shanghai
- US-qualified attorney with a background in computer science & engineering
- Cybersecurity & Data Compliance Counsel

YOUR CONTACT

REACH OUT

MAILING ADDRESS

Crystal Century Plaza, Suite 20C

567 Weihai Road, SHANGHAI

EMAIL ADDRESS

info@dawo-lf.com

PHONE NUMBER

021-6288 8682

Scan to follow our updates

Teneo®

The Global CEO Advisory Firm

Protecting Reputational Assets

- Crisis Preparedness and Management

September 18, 2020

About Teneo

The Global CEO Advisory Firm

Teneo is the global CEO advisory firm.

Working exclusively with the CEOs and senior executives of the world's leading companies, Teneo provides strategic counsel across their full range of key objectives and issues. Our clients include a significant number of the *Fortune* 100 and FTSE 100, as well as other global corporations.

Integrating the disciplines of strategic communications, investor relations, digital advisory, diversity & inclusion, management consulting, physical & cyber risk advisory, financial advisory, corporate governance advisory, political risk advisory, and talent advisory, Teneo solves for the most complex business challenges and opportunities.

Teneo's Global Reach & Asia Presence

Teneo is comprised of over 800 professionals located in 21 offices in key markets around the world. In Asia, Teneo has a team of over 50, operating from the strategic hubs of Hong Kong, Beijing, Shanghai, Singapore and Sydney. We serve clients across the region's diverse countries and markets.

Teneo's Core Services

Strategy & Communications Advisory

Advisory focused on managing reputation and protecting and enhancing shareholder value.

Capital Advisory

Leading global independent investment bank that provides innovative, unconflicted strategic advise.

Risk Advisory

Advisory focused on helping corporations anticipate and mitigate risks associated with geopolitics, physical security and cybersecurity.

Management Consulting

Advisory focused on strategic decision-making and business plan implementation, to help companies fully realize their business goals.

A Changing Landscape

Overall Observations

Narrative is strictly controlled by government, considering the fact that relevant laws are vague and Chinese government's desire to maintain momentum in tech industry

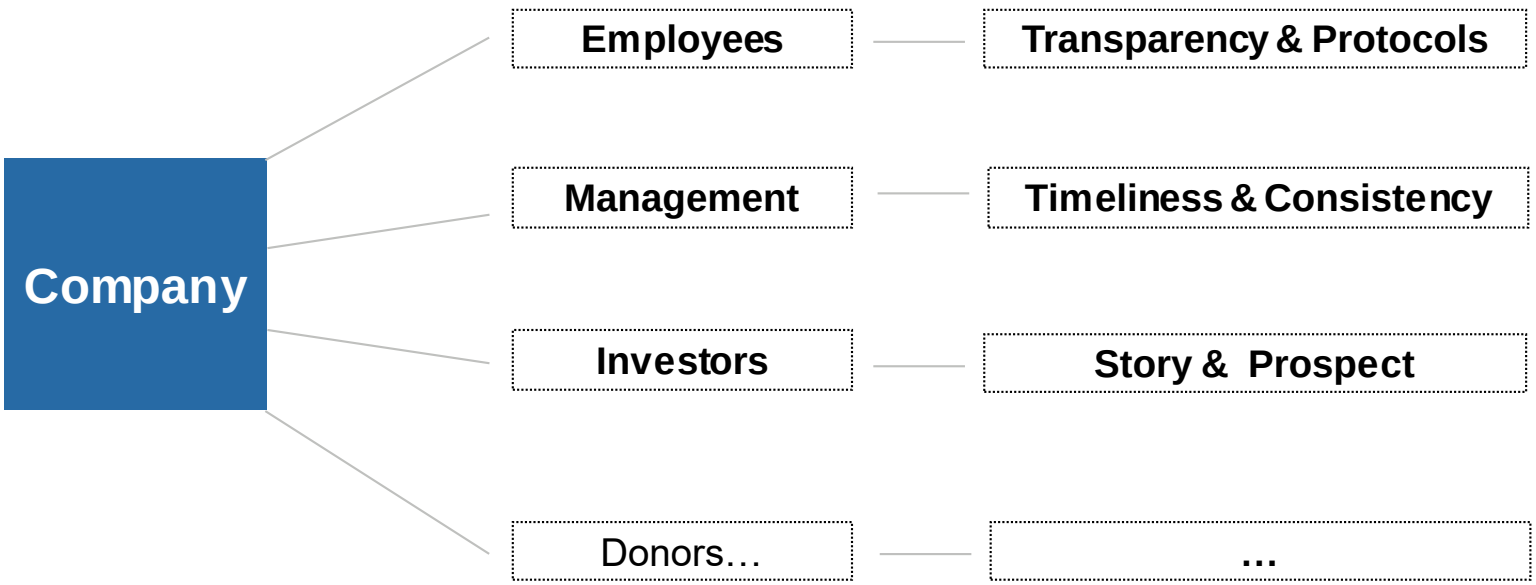
A company's profile in China is facing unprecedented risks as Chinese government responds to challenges on an international stage in a faster and more aggressive manner

An increasing number of companies, Chinese or foreign, are finding themselves **being caught in geopolitical disputes**

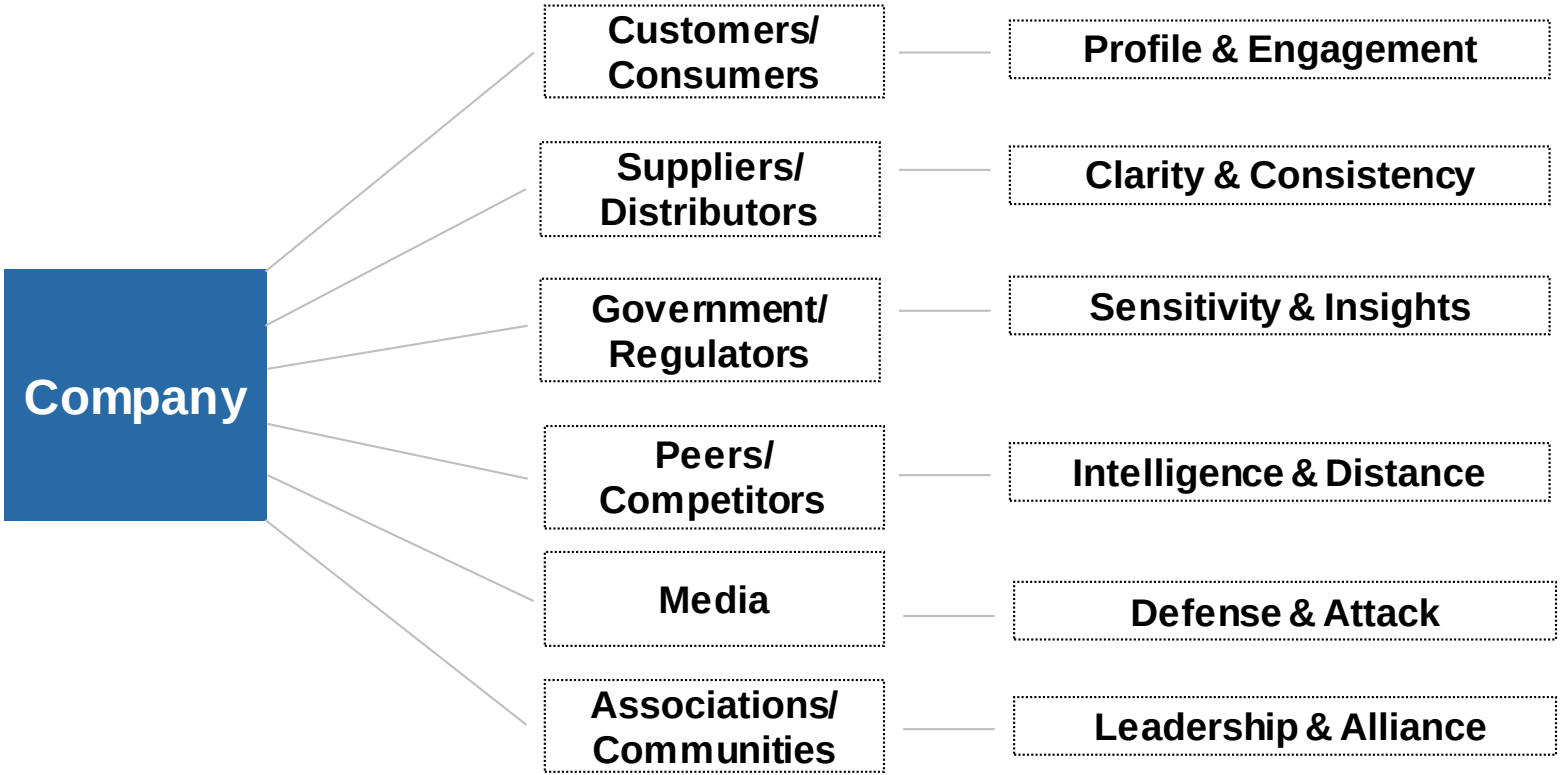
A company's **presence on social media** and its management team and employees' **remarks on social media** have more impactful ramifications than ever

Key Stakeholders and Related Communication

Internal Stakeholders

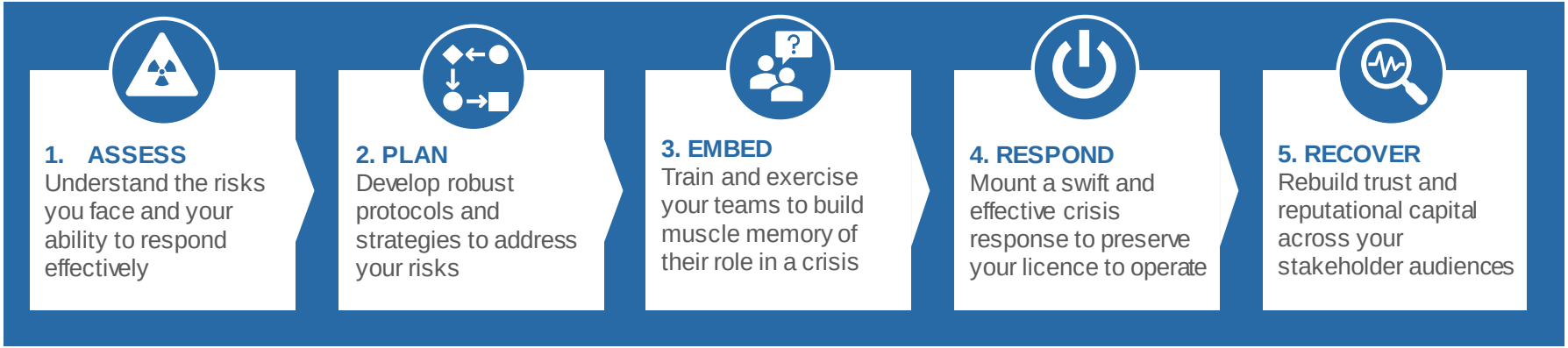


External Stakeholders



Approach to Risks and Crises

Five-step Approach



1. Assess

A thorough assessment of risk is an essential foundation for effective crisis planning. A company needs to identify and quantify their level of operational, financial and reputational risk exposure, and understand how well-equipped they are to mitigate and manage their current levels of risk.

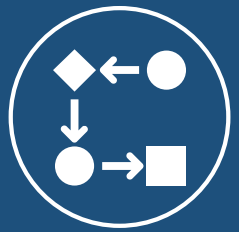
The company needs to assess where an organisation's risks are located; the types of risk; what impact they would have on the business if they crystallised; and what likelihood they have of materialising.

GEOPOLITICAL RISK

REPUTATION RISK

CAPABILITY AND READINESS

2. Plan



A company needs to develop targeted action plans that allow teams to close gaps in preparedness and develop mitigation strategies focused on their areas of greatest vulnerability.

The plans can be applied to a variety of situations, including on-going issues management, preparations for a major product launch or business acquisition, shareholder activism threat or a full-scale crisis.

CRISIS PLAN AND PROTOCOL CREATION

ISSUE OR RISK SPECIFIC PLANS

FUNCTION DESIGN AND DEVELOPMENT

3. Embed

To operate effectively, crisis plans must be fully understood and embedded before a crisis breaks.

The teams involved in a crisis response should understand – and be practised in executing – their roles.

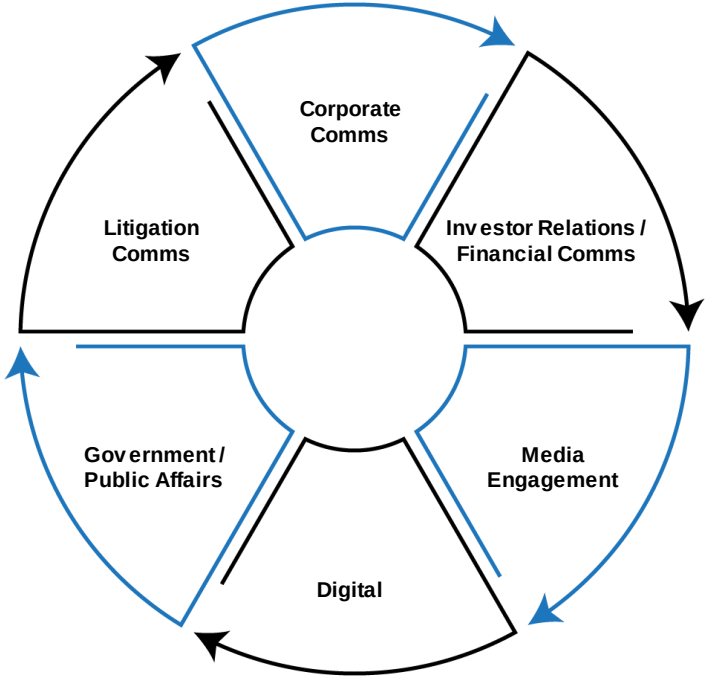
CRISIS TRAINING:

- Media training for senior leaders and spokespeople
- Crisis leadership coaching
- High stakes conversation coaching
- Preparation for parliamentary committees and other high profile political events
- Team exercises and drills
- Role-specific training
- Crisis exercises and simulations

4. Respond

During a crisis event, an organisation might need a full range of support, from senior counsel to message creation and crisis media management.

Companies need to fight to maintain credibility during a crisis. Holistic crisis response strategies will ensure alignment with legal and core business imperatives.



5. Recover

All crises end. And when they do, a company needs to assess how effectively they managed the situation and strengthen their crisis governance, protocols, policies, skills, assets and resources.

If a crisis occurred because of a systemic or cultural issue, a company needs to develop and implement change management and culture change programmes to tackle the situation head-on.

Stakeholders perception audits and insights inform reputation recovery strategies to rebuild trust and relationships with employees, customers, stakeholders, regulators and other audiences.

Reputation Rebuilding

Financial Recovery

Organizational Redesign

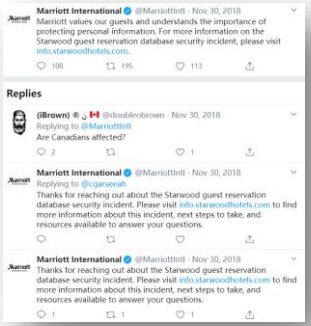
Case Studies

Marriott Data Breach

Nov. 30, 2018

Marriott International announced in a **press release** that a breach of its Starwood guest reservation database exposed the personal information of up to 500 million people. The hackers accessed people's names, addresses, phone numbers, email addresses, passport numbers, dates of birth, gender.

Arne Sorenson, **Marriott's President and Chief Executive Officer apologized**, "We deeply regret this incident happened. We fell short of what our guests deserve and what we expect of ourselves. We are doing everything we can to support our guests, and using lessons learned to be better moving forward."



Marriott International **Twitter account and social media platforms** emphasized the message that "Marriott values guests and personal data" and directed the online requests/questions to streamlined process – **dedicated website and call center.**

Marriott Data Breach

CEO Interviews

Weibo Data Breach

March 19, 2020

Alibaba's former security chief Wei Xingguo claimed on Weibo that data on millions of Weibo users, including his own contact details, had been leaked online. Wei's statement triggered a **public outcry online**. Chinese media and international media reported that data of 538 million Weibo users are available for sale on the dark web.

Weibo issued a **statement**, in which it admitted to the data leak and said "the leak did not involve ID numbers or password and did not affect the operation of Weibo…using the same password on different platforms will put Weibo users at greater risk of their personal information being stolen."

Ministry of Industry and Information Technology summoned representatives from Weibo to a meeting and ordered them to enhance data security.