



Guidance Document

Cyber Security in Emerging Geographies

Prepared by the
Chemical Information Technology Center (ChemITC[®])
Chemical Sector Cyber Security Program
Emerging Geographies High Interest Topic (HIT) Team

September 2009

Legal and Copyright Notice

IMPORTANT: *This document is presented by the Chemical Information Technology Center (ChemITC®) of the American Chemistry Council (ACC) to assist information security professionals already sophisticated and experienced in the area of cyber security. The Chemical Sector Cyber Security Program is a strategic program of ChemITC.*

ChemITC has taken reasonable measures to develop this document in a fair and unbiased manner for the purpose of outlining key issues relating to evolving cyber security practices, concerns and needs within emerging geographies. Examples identified in the document are intended to illustrate the principles discussed and represent only some available options. The identification of any particular practice, supplier, product or other information in the document does not constitute an endorsement, guarantee or warranty by ACC, ChemITC or any of their members. The document provides only general guidance to stimulate further thinking and analysis; information provided in the document is in no way intended to establish a standard, legal obligation or preferred option for any practice or supplier.

Although the information provided in this document is offered in good faith, and believed accurate based upon information available to preparers of the document, neither ACC, ChemITC, nor their individual member companies or employees, makes any warranty or representation, either express or implied, with respect to the accuracy or completeness of the information contained herein; nor do these organizations and individuals assume any liability or responsibility for reliance on any product, process or other information disclosed. None of the aforementioned parties shall be liable for any loss, damage, or claim with respect to this document, all such liabilities, including direct, special, indirect or consequential damages, are expressly disclaimed.

New information may be developed subsequent to publication that affects the document's completeness or accuracy. ACC and ChemITC assume no responsibility to revise the document to reflect any information that becomes available after its publication. Notwithstanding, because this document may be revised periodically, the reader is advised to visit the ChemITC Web site (www.chemitc.com) to obtain the most current version.

This document is protected by copyright. ACC hereby grants a nonexclusive, royalty-free license to reproduce the document provided: copies of the work are not sold and the document is reproduced in its entirety without alterations.

Table of Contents

Table of Contents	3
Introduction	4
Purpose and Scope.....	4
Document Structure	4
Overview	5
Why Emerging Geographies?	5
Methodology.....	5
Cyber Security Key Issues	5
Intellectual Asset Protection	5
U.S. Export Compliance	8
Data Privacy	10
Corruption Index.....	11
Cryptography.....	11
Regulatory – Laws and Judicial Environment	13
Overview by Country	15
Themes	15
Further Study Required	15
Differences with Established Geographies.....	15
Collected Examples.....	15
Timeline/Trend for the Issue.....	15
Business Environments.....	16
Mergers, Acquisitions and Divestures (MA&D)	16
Outsourcing	16
Joint Ventures (JV).....	16
Supply Chains	16
Shared Service Centers	16
Appendix A: Glossary of Terms	17
Appendix B: Useful References	18
Export Control References.....	18
Data Protection Principles.....	18
Data Protection Laws Around the World	18
Asia	18
Eastern Europe	18
Middle East.....	18
South America.....	18
Cryptography References	18
Appendix C: Emerging Geographies Workbook	19
Appendix D: Pharmaceutical Counterfeiting Analysis	20

Introduction

Purpose and Scope

As global chemical companies expand into regions of the world outside of the United States and Western Europe, there is a growing need to understand the evolving cyber security issues in these new locations. ChemITC formed a high interest topic (HIT) team in October 2007 to examine this need. This team acted on behalf of ChemITC and included representatives from the information security organizations within Air Products and Chemicals, Ashland Incorporated, The Dow Chemical Company and Shell Chemicals, as well as a ChemITC Affiliate member representative from Deloitte LLP.

At the project onset, the team identified three key objectives.

- Creation of a primer document to support and include project/development and support processes focusing on:
 - Generic understanding of evolving cyber security issues
 - Specific country elements where applicable
 - Risk assessment of highlighted issues
- Guidance on ways to address identified issues and/or directions on where to gain further help
- Highlight key issues not covered in this work that other Cyber Security Program teams may consider for further study

The research examined cyber security in the following world areas.

- Asia – China, India and Vietnam
- Eastern Europe – Poland, Romania and Russia
- South America – Argentina, Brazil and Mexico
- Middle East – Saudi Arabia

The research focused on business process enablement in the following areas.

- Manufacturing
- Shared services* (i.e., finance, human resources, IT, etc.)
- Supply chain
- Engineering
- Research and development

* Note = This includes outsourcing services

Document Structure

This document outlines why cyber security in emerging geographies should be of interest, the methodology used to examine key issues in these areas and the six areas of cyber security that were included in scope. The document then defines each of these six areas, outlines the results of findings, includes links to key public sources of information and highlights key learnings.

The Overview by Country section references the workbook which was created to give a high-level relative assessment across all countries within the scope of the analysis. This was done using publicly available comparative measures.

Overview

Why Emerging Geographies?

Over the last decade or so, a major shift of the world's manufacturing base has moved production to Asia and other lower-cost regions. The chemical sector is part of this movement; most of the ChemITC membership has established or is in the process of establishing a presence in these regions.

Emerging geographies are associated with a perception of higher risk. The trend toward moving production to lower-cost areas has given rise to cyber security concerns for companies in many industries, including chemical businesses and the information security professionals they employ. This document is the result of a search for data to help validate or disprove these concerns.

Methodology

To examine cyber security concerns in emerging geographies, a list of evolving cyber security issues was created and prioritized based on level of interest. These six key issues are listed in the following section. A workbook was also created (see [Section 3](#) and [Appendix C](#)) to show a comparison across each country of various indicators within each area.

Cyber Security Key Issues

Intellectual Asset Protection

Definitions

Various terms are often used when discussing intellectual asset protection, but while they are all very similar, there are subtle differences between each. For the purposes of this report, the following definitions apply:

- **Intellectual capital** – All knowledge, whether written or not (i.e., in a person's head), that the company possesses
- **Intellectual assets** – Written knowledge that the company possesses
- **Intellectual property** – Knowledge with legal ownership (e.g., patents, trade secrets, etc.) that the company possesses

This paper focuses on intellectual asset protection as opposed to the more specific intellectual property (IP) protection.

Intellectual Asset Loss

There is a limited amount of industry-wide intellectual asset loss data and statistics pertaining specifically to the chemical and process manufacturing industry. In fact, most data and research surrounding intellectual asset loss concerns piracy and counterfeiting in the digital media and entertainment industries. However, some data is available regarding intellectual asset loss within the life science and pharmaceutical industries. While the pharmaceutical and chemical industries have many significant differences, they do have common concerns over intellectual asset loss, including the need to protect proprietary production methods, chemical formularies or equipment designs from being compromised. As such, available life science and pharmaceutical data was considered as a proxy for the potential risks of intellectual asset loss in the chemical industry.

Collecting data related to chemical industry intellectual asset loss can be challenging. A 2007 Deloitte and Touche analysis of pharmaceutical counterfeiting provides relevant data on this topic for an industry largely similar to the chemical industry. [Appendix D](#) illustrates the various figures and estimates for counterfeiting and parallel importation of pharmaceutical goods. The figures are derived from sources of information regarding counterfeiting, grey market and product diversion of pharmaceutical goods, such as the World Health Organization and the U.S. Food and Drug Administration. In some instances, the statistics can be staggering. For example, an estimated percentage of drugs that are either fake or adulterated in Nigeria have now reached as high as 70 percent.

Key Learning: While intellectual asset loss is a concern within the chemical industry, there is a lack of data to support the quantification of its magnitude. Without further study on this topic, chemical companies may often have to rely on educated guesses or rough estimates based on observations in other industries that have more thoroughly studied the issue.

Cultural Aspects

This section intends to provide an overall view of the cultural climate regarding intellectual asset protection in the countries researched. In considering this topic, a number of questions were asked including:

1. Is the act of appropriating intellectual assets considered “wrong” in the country?
2. Is appropriation of intellectual assets rewarded rather than punished?
3. Do the people feel entitled to the knowledge?
4. Are the intellectual assets of other companies readily available in the local (or cyber) market in this country?
5. Is there legal recourse? How long does it take a case to come to trial?
6. Is the situation getting better or worse?

The goal of the research was to find objective, fact-based examples to support a position on the state of the cultural climate in each country regarding intellectual asset protection. On one side, the information available tended to be both anecdotal (a retelling of someone’s corporate experience from one perspective only) and sensational (tabloid-quality hyperbole about the magnitude of the theft or loss). To support the opposing view, a good deal of press discusses the situation emerging geographies face with regard to intellectual capital development. This material points to the fact that these countries simply cannot catch up with the rest of the world in a timely manner unless they build on foundations already developed. For example, they must ‘take’ intellectual assets rather than develop them in order to be competitive with developed nations in the near term.

In studying this information, it became obvious that available examples were mostly subjective rather than objective. Thus, the research and opinions of the World Trade Organization (WTO) and the Office of the United States Trade Representative (USTR), two recognized organizations dedicated to fair trade practices, was used. These organizations have the staff and resources to track legislation, monitor specific court cases and compile trend reports over time. They also consider it part of their charter to provide an informed opinion on the cultural aspects of intellectual asset protection by country. Both organizations provide summary opinions, as well as detailed information and links, so the reader can research as much or as little as required. The USTR is especially conservative; however, they are consistent in this approach over time.

World Trade Organization (WTO)

All of the countries in scope except Russia belong to the World Trade Organization and are therefore subject to its regulations and governance. The WTO is a global organization dedicated to enabling and enhancing trade between nations. Core to the organization are WTO Agreements, which are negotiated by the member nations and signed into law in their respective countries. Trade Related Aspects of Intellectual Property Rights (TRIPS) is the agreement dedicated to the protection of intellectual assets. The agreement addresses five broad topics:

- Application of intellectual property agreements to basic trading principles
- How to adequately protect intellectual property rights
- Enforcement of intellectual property rights
- Dispute settlement between member countries
- Transitional arrangements during the cutover period

Elements of intellectual property covered under this agreement include:

- Copyrights
- Trademarks
- Geographical indicators (e.g., champagne, cheddar, etc.)
- Industrial design
- Patents
- Integrated circuit layout designs
- Undisclosed information and trade secrets
- Technology transfer between member nations

World Intellectual Property Organization (WIPO)

The World Intellectual Property Organization is a specialized agency of the United Nations. Its mission is to develop a balanced and accessible international intellectual property (IP) system, which rewards creativity, stimulates innovation and contributes to economic development while safeguarding the public interest.

WIPO was established by the WIPO Convention in 1967 with a mandate from its member states to promote the protection of IP throughout the world through cooperation among states and in collaboration with other international organizations. Its headquarters are in Geneva, Switzerland.

The following table points to country profiles outlining relevant legislation and WIPO treaties:

Country	Country Profile
Argentina	http://www.wipo.int/members/en/details.jsp?country_id=8&country_code=AR
Brazil	http://www.wipo.int/members/en/details.jsp?country_id=23&country_code=BR
China	http://www.wipo.int/members/en/details.jsp?country_id=38&country_code=CN
India	http://www.wipo.int/members/en/details.jsp?country_id=80&country_code=IN
Mexico	http://www.wipo.int/members/en/details.jsp?country_id=123&country_code=MX
Poland	http://www.wipo.int/members/en/details.jsp?country_id=141&country_code=PL
Russia	http://www.wipo.int/members/en/details.jsp?country_id=147&country_code=RU
Romania	http://www.wipo.int/members/en/details.jsp?country_id=146&country_code=RO
Saudi Arabia	http://www.wipo.int/members/en/details.jsp?country_id=149&country_code=SA
Vietnam	http://www.wipo.int/members/en/details.jsp?country_id=185&country_code=VN

Office of the United States Trade Representative (USTR)

The Office of the United States Trade Representative publishes the Special 301 Annual Review, which provides detailed information on the state of intellectual property rights protection in 87 countries. Most recently published for the year ending December 2007, the Special 301 Annual Review contains the Watch List and the Priority Watch List.

The Watch List includes countries where the protection of intellectual property rights is lacking or not up to standard. Commentary is included as to whether the specific climate is improving or declining. U.S. recommendations for improvement and focus are also included. Countries on the 2007 Watch List include Brazil, Mexico, Poland, Romania and Saudi Arabia.

The Priority Watch List highlights countries where violations are extreme and the regulation of intellectual property protection is either non-existent or severely compromised. Narrative is included itemizing the types of violations and progress made to date. An analysis is often provided comparing the past state of compliance with the present state. Countries on the 2007 Priority Watch List include Argentina, China, India and Russia.

The Special 301 Annual Review also provides an executive summary highlighting positive improvements by geography. A notorious markets section is also included identifying both virtual and physical marketplaces for pirated intellectual property.

Stop Fakes

Stop Fakes is a joint effort between several U.S. agencies including the Commerce Department, State Department and Department of Homeland Security. Notable on this site are the IPR toolkits, which provide information about intellectual property rights environments on a per country basis. Additionally, the toolkits walk the reader through the process of setting up business operations in the referenced country from an intellectual property protection perspective.

U.S. Export Compliance

One factor that comes into play as U.S. companies conduct business in emerging geographies is adhering to export control regulations. For the purpose of this research, the focus in this area is on U.S. export laws and regulations impacting cross-border movement and/or transfer of the following:

- Goods
- Services
- People
- Technology
- Software

Corporations should ensure they are conducting business in a way that complies with all relevant regulations. In the case of export control, these regulations are complex and difficult to interpret, compounding the challenge of ensuring compliance by all parties regardless of transaction location or the nationality of the parties involved.

Figure 2: Primary Export Control Regulations

A number of regulations related to export control apply, depending upon the type of business transaction. Links to additional information can be found in [Appendix B](#).

Regulations	Control Areas
Export Administration Regulations (EAR)	Dual-use items and technology, cryptography
International Traffic in Arms Regulations (ITAR)	Military, space
Department of Treasury – Office of Foreign Assets Control (OFAC)	Embargoes
Department of Justice – Drug Enforcement Administration (DEA)	Narcotics and dangerous drugs, precursors and solvents

Figure 3: Other U.S. Agencies and Scope of Control

Agency	Control Areas
Environmental Protection Agency	Toxic substances (e.g., insecticides, pesticides, listed chemicals)
Department of Agriculture	Seeds, plants, soils
Department of Energy	Nuclear weapons/technical data, nuclear materials, natural gas/electric power
Nuclear Regulatory Commission	Nuclear equipment and materials
Department of Interior	Endangered fish and wildlife
Department of Transportation	Prohibition of movement of American Carriers
Food and Drug Administration	Food, drugs, biological products, medical devices

The Australia Group (AG)

The Australia Group, an informal agreement between 34 countries including Poland, Romania, Argentina, United Kingdom and the United States, is the main multi-national agreement that covers export control. The main objective of the AG is to ensure that dual-use chemicals exported by these countries do not contribute to the spread of chemical weapons. AG countries may receive chemical weapons precursors or technology for production or disposal without a license.

Some countries require a license for export of common chemical processing equipment and related technologies because they are perceived to possess an elevated risk regarding export control concerns. These countries are not members of the AG, and as such are not afforded the same freedoms relative to export control. They include:

- Brazil
- China
- India
- Mexico

- Russia
- Saudi Arabia
- Vietnam

Key Learning: It is perceived that there are higher risks and the possibility of more issues when doing business in these countries; hence greater compensating controls must be present.

Data Privacy

Data privacy is emerging as a major issue around the world. It is important to distinguish between data privacy and data protection.

According to the UK's Calcutt Committee in the 1970s, data privacy is defined as the right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information.

Data protection, however, is defined as interpreting privacy in terms of management of personal information.

In examining this issue, three areas were examined.

- Data protection principles
- Data protection legislation
- Data protection enforcement

There are five major sets of data protection approaches that are applied around the world.

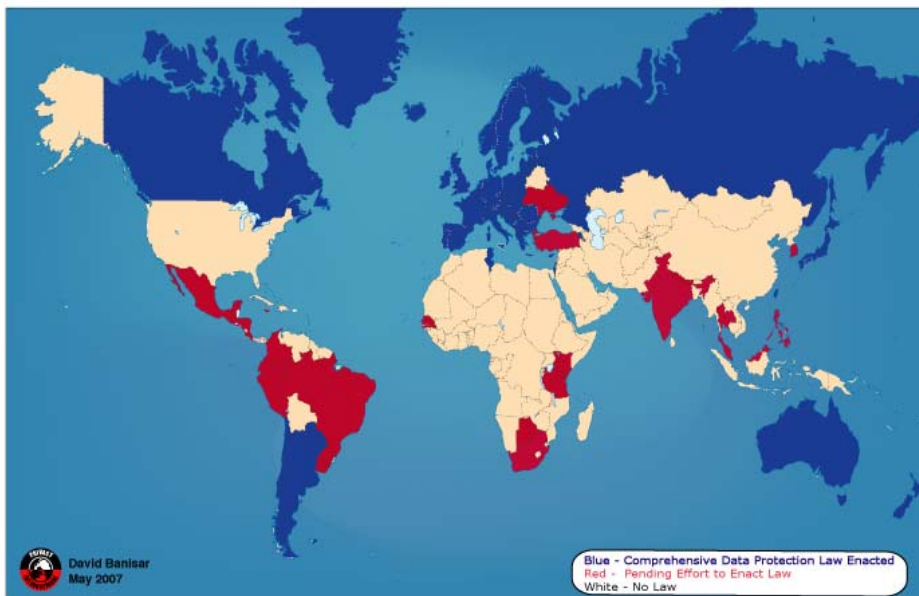
- Asia-Pacific Economic Cooperation
- European Union (EU) Directive on Data Protection (95/46/EC)
- Generally Accepted Privacy Principles
- Organisation for Economic Co-operation and Development (OECD) Working Party on Information Security and Privacy (WPISP)
- Safe Harbor

These approaches share the following common themes. Data must be:

- Obtained fairly and lawfully
- Used only for the original specified purpose
- Adequate, relevant and not excessive to purpose
- Accurate and up-to-date
- Accessible to the subject
- Kept secure
- Destroyed after its purpose is completed

Of the countries in scope, Argentina, Poland and Romania have the most protective legislation and are based on European Union directives and/or EU data protection principles. Of the other countries, Brazil and Russia have data protection legislation in place as well. However, the Russian enforcement regime does not appear to be as rigorous as some other world areas. India and Mexico have legislation pending and there is some connected legislation in China. At this time, data protection information could not be found for Saudi Arabia or Vietnam.

Data Protection Laws Around the World



Key Learning: Data privacy/protection is being increasingly acknowledged as an issue in most countries, with the need to respond becoming key to future development for some of the countries that provide outsourcing services. Consequently, the situation is improving in most of the countries researched.

Corruption Index

According to an annual survey by the Berlin-based organization Transparency International (TI), Finland, Denmark and New Zealand are perceived to be the countries with the least amount of political corruption, and the political environments of Somalia and Myanmar are perceived to be the most corrupt. The index defines corruption as the abuse of public office for private gain and measures the degree to which corruption is perceived to exist among a country's public officials and politicians. It is a composite index, drawing on 14 polls and surveys from 12 independent institutions that gather the opinions of business people and country analysts. Only 180 of the world's 193 countries are included in the survey, due to an absence of reliable data from the remaining countries. The scores range from 10 (Highly Ethical) to zero (Highly Corrupt). Transparency International considers a score of 5.0 the borderline distinguishing countries that do and do not have a serious corruption problem.

The corruption index in the related workbook (see [Appendix C](#)) outlines two items:

- The corruption index score
- The relative ranking out of 180 countries

Key Learning: One of the best ways to deal with potential issues in corruption is to reinforce company Code of Conduct and Appropriate Use policies through training and testing understanding.

Cryptography

When discussed in the context of information technology, cryptography is the conversion of data into a secret code for transmission over a public network. Today, most cryptography is digital

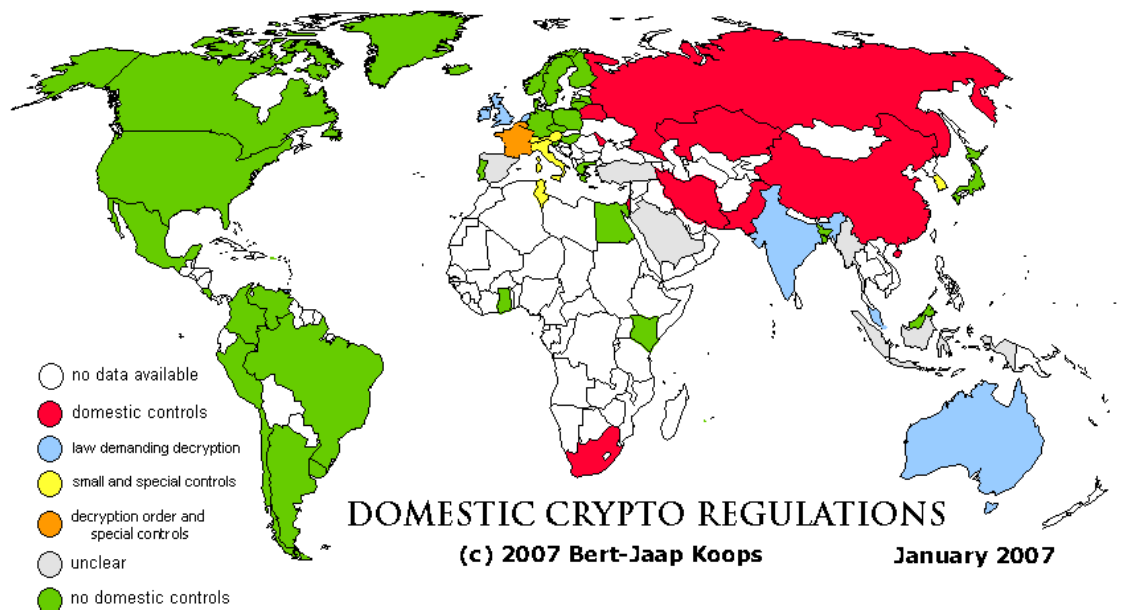
and the original text ("plaintext") is turned into a coded equivalent called ciphertext via an encryption algorithm. The ciphertext is decrypted at the receiving end and turned back into plaintext.

The encryption algorithm uses a "key," which is a binary number typically between 40 and 256 bits in length. The greater the number of bits in the key (cipher strength), the more possible key combinations and the longer it would normally take to break the code. The data is encrypted or locked by combining the bits in the key mathematically with the data bits. At the receiving end, the key is used to unlock the code and restore the original data.

The following international organizations and agreements set the standards and guidelines and govern the approach to cryptography globally.

- Wassenaar Arrangement / COCOM
- Council of Europe
- European Union
- Organisation for Economic Co-operation and Development (OECD)
- Business Government Forum

The use of cryptography can be an important tool for organizations seeking to prevent unauthorized use or disclosure of their confidential business information. Notwithstanding because the technology can also be used for unlawful purposes, and because several countries do not afford high levels of individual privacy, some governments restrict use of the technology. The lightest cryptography controls are in Argentina, Brazil, Mexico, Poland and Vietnam. There are decrypt laws in India and the most stringent controls are in China, Russia and Saudi Arabia.



Prof.dr. Bert-Jaap Koops is professor of regulation and technology at the Tilburg Institute for Law, Technology and Society (TILT) at Tilburg University, the Netherlands. His world renowned Crypto Law Survey is a useful reference and starting point for further detailed research in cryptography.

Key Learning: Certain governments included in this analysis will continue to legislate in this area

in order to ensure that they can deal with malicious intent either from other governments or individuals. It is important to engage legal contacts with knowledge of specific countries to ensure that legislation is adhered to and that adequate controls are put in place.

Regulatory – Laws and Judicial Environment

Four key sources of information on global laws and judicial environments were researched. They are identified and briefly described in the table below.

Figure 4: Laws and Judicial Environment

Link	Source	Description
Global Integrity	Independent information on governance and corruption	The Global Integrity Index assesses the existence and effectiveness of anti-corruption mechanisms that promote public integrity. More than 290 discrete integrity indicators generate the Integrity Index. They are organized in six key categories and 23 sub-categories. They are prepared by a lead researcher in the country and then blindly reviewed by additional in-country and external experts. The Integrity Indicators assess the existence of laws, regulations and institutions designed to curb corruption, as well as their implementation and the access that average citizens have to those mechanisms.
Index of Economic Freedom	The Heritage Foundation and <i>The Wall Street Journal</i>	Ten specific factors are measured and averaged equally into a total score. Each one of the 10 freedoms is graded using a scale from 0 to 100, where 100 represents maximum freedom. A score of 100 signifies an economic environment or set of policies most conducive to economic freedom. The 10 component freedoms are: business freedom, trade freedom, fiscal freedom, government size, monetary freedom, investment freedom, financial freedom, property rights, freedom from corruption and labor freedom.
Doing Business	International Finance Corporation <i>World Bank Group</i>	The Doing Business project provides objective measures of business regulations and their enforcement across 178 countries and selected cities at the sub-national and regional level. It provides information on ease of starting a business, dealing with licenses, employing workers, registering property, getting credit, protecting investors, paying taxes, trading across borders, enforcing contracts and closing a business, with comparisons in each area between 2007 and 2008 rankings.
World Legal Information Institute	The World Legal Information Institute	The World Legal Information Institute is a collaborative project of Legal Information Institutes including Australian, British and Irish, Canadian, Hong Kong, Cornell and Pacific Islands Legal Information Institutes, Wits University School of Law and other organizations. It is a free, independent and non-profit global legal research facility developed collaboratively. It resources 891 databases from 123 countries via the Free Access to Law Movement.

Figure 5 provides a summary of the information obtained from the identified sources for the

countries within the scope of this report. Due to the extensive amount of information accessible from the World Legal Information Institute, the table simply identifies whether information on the specified country is available. Interested parties can directly access the World Legal Information Institute¹ to research topics of interest.

Figure 5: Laws and Judicial Environment Information Available by Country

Country	Global Integrity Index 2006		Heritage Foundation Index of Economic Freedom 2008		Doing Business		World Legal Information Institute
	Score (scale of 100)	Overall Rating	Rank of 157	Freedom (percent)	2007 Rank of 175	2008 Rank of 178	Information available? (Y/N)
Asia							
China	No data	No data	126	52.8 Mostly unfree	92	83 ↑	Y
India	75	Moderate	115	54.2 Mostly unfree	132	120 ↑	Y
Vietnam	47	Very weak	135	49.8 Repressed	94	91 ↑	Y
Eastern Europe							
Poland	No data	No data	83	59.5 Mostly unfree	68	74 ↓	No databases – catalog only
Romania	86	Strong	68	61.5 Moderately free	55	48 ↑	Y
Russia	63	Weak	134	49.9 Repressed	112	106 ↑	Y
South America							
Argentina	79	Moderate	108	55.1 Mostly unfree	101	109 ↓	Y
Brazil	73	Moderate	101	55.9 Mostly unfree	113	122 ↓	Y
Mexico	65	Weak	44	66.4 Moderately free	41	44 ↓	Y
Middle East							
Saudi Arabia	No data	No data	60	62.8 Moderately free	33	23 ↑	Y

Key Learning: This is a very dynamic area and any company wishing to enter into business in these countries should ensure they conduct appropriate due diligence with regards to the various pieces of legislation outlined above.

¹ World Legal Information Institute - <http://www.worldlii.org/>

Overview by Country

Figure 6 provides a snapshot of the workbook accompanying this report, which summarizes report findings, shows the relative assessment of the six cyber security issues covered by country and compares them with established geographies, including the United States and United Kingdom.

Figure 6: Overview by Country

FINAL	Asia			Eastern Europe			South America			ME	Established	
	China	India	Vietnam	Poland	Romania	Russia	Argentina	Brazil	Mexico	Saudi Arabia	USA	UK
1 Intellectual Asset Protection												
Cultural aspects	Priority Watch List	Priority Watch List	Watch List	Watch List	Watch List	Priority Watch List	Priority Watch List	Watch List	Watch List	Watch List		
2 US Export Compliance												
	Requires License	Requires License	Requires License	Australia Group	Australia Group	Requires License	Australia Group	Requires License	Requires License	Requires License	Australia Group	Australia Group
3 Data Privacy												
DP Principles	APEC	GAPP	APEC	EU	EU	EU	EU	Ibero-American	EU/APEC	No Info	GAPP	EU
DP Regulations	Some	Pending	No Info	Yes	Yes	Yes, but inactive	Yes	Yes	Pending	No Info	Some	Yes
4 Corruption Index (10 to 0)												
Ranking (out of 180)	3.5	3.5	2.6	4.2	3.7	2.3	2.9	3.5	3.5	3.4	7.2	8.4
	72=	72=	123	61	69	143	105	72=	72=	79	20	12
5 Government views on cryptography												
	Controls	Decrypt Laws	No Controls	No Controls	No Data	Controls	No Controls	No Controls	No Controls	Controls	No Controls	Decrypt Laws
6 Regulatory – Laws & Judicial Environment												
Ranking out of 157	126	115	135	83	68	134	108	101	44	60	5	10

Themes

Further Study Required

It is worth noting that there are no straight-forward answers to questions about cyber security in these emerging geographies. The data provided here is a starting point to gather additional relevant information key to business. Companies should ultimately rely on good business judgment to influence direction.

Differences with Established Geographies

Figure 6 compares the relative assessments with established geographies to guide decisions and assumptions made in dealing with cyber security in emerging geographies. Please remember that a layer of company culture is added to the mix as a business works through these issues.

Collected Examples

The accompanying workbook outlines the details behind the summary table above and includes a worksheet for each of the cyber security issues, outlining examples of and links to further information for each issue.

Timeline/Trend for the Issue

Creation of this document began in 2008 and contains data from 2006 and 2007. It is important to consider trending for the particular cyber security issue of interest, as well as the country

being researched. Where possible, links to active sites are provided.

Business Environments

Mergers, Acquisitions and Divestures (MA&D)

This document seeks to provide guidance in developing an approach to due diligence and/or information risk assessment. It is important to consider the above cyber security issues in the context of their impact on the overall risk of doing business in a particular country. Broader information security management issues should be addressed as part of that exercise.

Outsourcing

From an outsourcing perspective, it is important to address broader information security issues from a people, process and technology viewpoint. When looking at risk mitigation, it is important to understand that in most cases ownership of risk and liability stays with the company and cannot be outsourced with other service provisions.

Joint Ventures (JV)

Joint venture partners in emerging geographies will need to be assessed during due diligence for their knowledge of the broad issues related to cyber security in their countries and region. Depending on percent ownership and/or who has control of the JV, ownership of risk and liability typically goes with the majority partner.

Supply Chains

As with outsourcing and joint ventures, risk and liability ownership considerations should be addressed. Intellectual asset protection and U.S. export compliance are key areas of risk.

Shared Service Centers

Note that issues related to Shared Service Centers may potentially be linked to guidance provided in the sections on outsourcing and JVs above. A key area of focus is in data privacy/protection.

Appendix A: Glossary of Terms

- **Cryptography** – The conversion of data into a secret code for transmission over a public network.
- **Data privacy** –The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information.
- **Data protection** – Interpreting privacy in terms of management of personal information.
- **Export control regulations** – Federal laws that prohibit the unlicensed export of certain commodities or information for reasons of national security or protections of trade.
- **Intellectual assets** – Written knowledge that the company possesses.
- **Intellectual capital** – All knowledge, whether written or not (i.e., in a person’s head), that the company possesses.
- **Intellectual property** – Knowledge with legal ownership (e.g., patents, trade secrets, etc.) that the company possesses.

Appendix B: Useful References

Export Control References

- [Department of Justice - Drug Enforcement Administration \(DEA\)](#)
- [Department of Treasury - Office of Foreign Assets Control \(OFAC\)](#)
- [Export Administration Regulations \(EAR\)](#)
- [International Traffic in Arms Regulations \(ITAR\)](#)
- [The Australia Group \(AG\)](#)

Data Protection Principles

- [Asia-Pacific Economic Cooperation](#)
- [European Union \(EU\) Directive on Data Protection \(95/46/EC\)](#)
- [Generally Accepted Privacy Principles](#)
- [Organisation for Economic Co-operation and Development \(OECD\) Working Party on Information Security and Privacy \(WPISP\)](#)
- [Safe Harbor](#)

Data Protection Laws Around the World

Asia

- [China](#)
- [India](#)

Eastern Europe

- [Poland](#)
- [Romania](#)
- [Russia](#)

Middle East

- [Saudi Arabia](#)

South America

- [Argentina](#)
- [Brazil](#)
- [Mexico](#)

Cryptography References

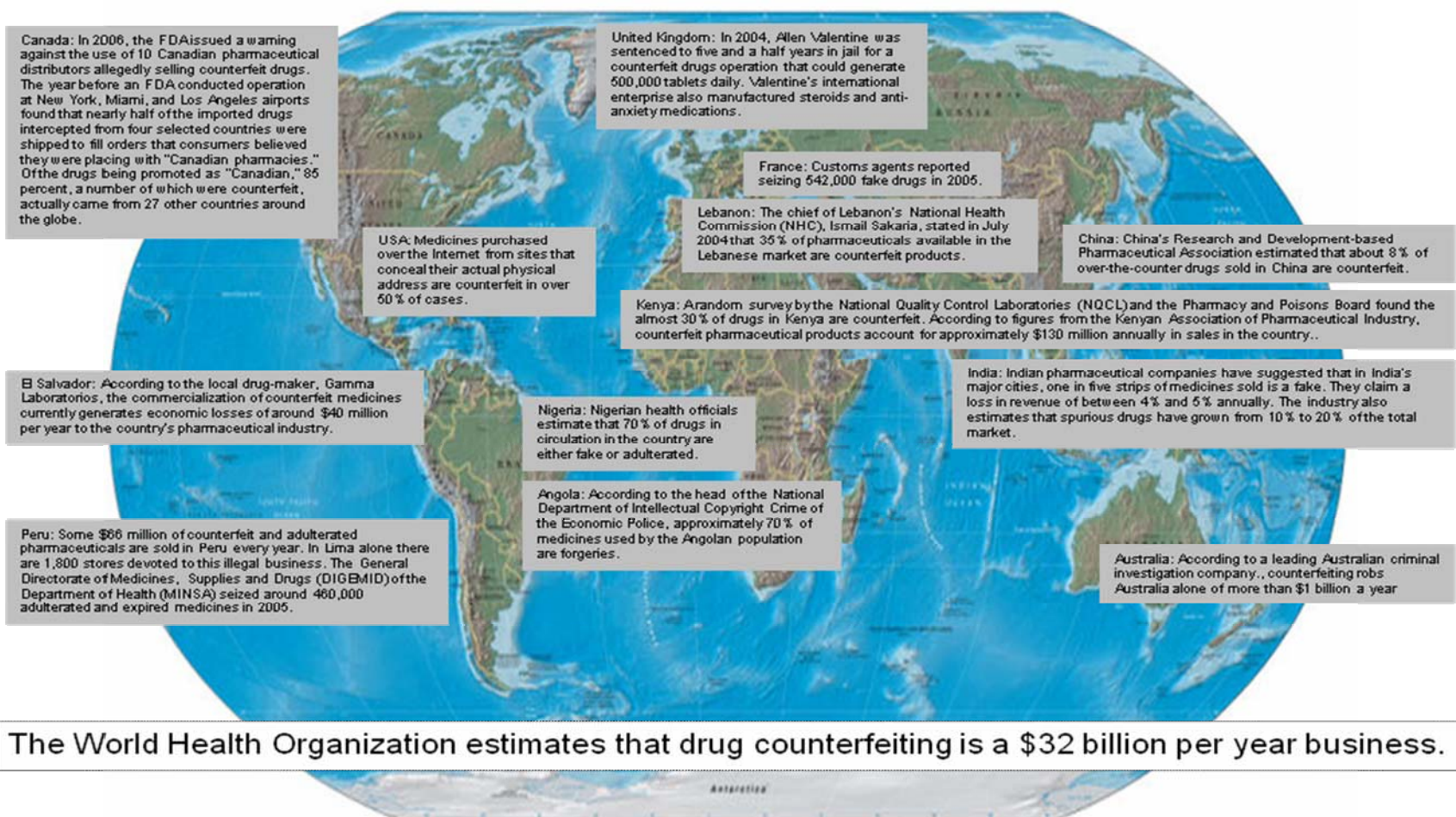
- [Crypto Law Survey](#)
- [Wassenaar Arrangement / COCOM](#)
- [Council of Europe](#)
- [European Union](#)
- [Organisation for Economic Co-operation and Development \(OECD\)](#)
- [Business Government Forum](#)

Appendix C: Snapshot of Emerging Geographies Workbook

FINAL	Asia			Eastern Europe			South America			ME	Established	
	China	India	Vietnam	Poland	Romania	Russia	Argentina	Brazil	Mexico	Saudi Arabia	USA	UK
1 <u>Intellectual Asset Protection</u>												
Cultural aspects	Priority Watch List	Priority Watch List	Watch List	Watch List	Watch List	Priority Watch List	Priority Watch List	Watch List	Watch List	Watch List		
2 <u>US Export Compliance</u>	Requires License	Requires License	Requires License	Australia Group	Australia Group	Requires License	Australia Group	Requires License	Requires License	Requires License	Australia Group	Australia Group
3 <u>Data Privacy</u>												
DP Principles	APEC	GAPP	APEC	EU	EU	EU	EU	Ibero-American	EU/APEC	No Info	GAPP	EU
DP Regulations	Some	Pending	No Info	Yes	Yes	Yes, but inactive	Yes	Yes	Pending	No Info	Some	Yes
4 <u>Corruption Index (10 to 0)</u>	3.5	3.5	2.6	4.2	3.7	2.3	2.9	3.5	3.5	3.4	7.2	8.4
Ranking (out of 180)	72=	72=	123	61	69	143	105	72=	72=	79	20	12
5 <u>Government views on cryptography</u>	Controls	Decrypt Laws	No Controls	No Controls	No Data	Controls	No Controls	No Controls	No Controls	Controls	No Controls	Decrypt Laws
6 <u>Regulatory – Laws & Judicial Environment</u>												
Ranking out of 157	126	115	135	83	68	134	108	101	44	60	5	10

Please note: ChemITC members may find the complete workbook on the [Cyber Security Program Work Space](#) on the American Chemistry Council's [MemberExchange](#).

Appendix D: Pharmaceutical Counterfeiting Analysis



Source: Pharmaceutical Counterfeiting Analysis for Client, Deloitte & Touche LLP, 2007