CYBERCRIME & SECURITY

Cybercrime & Security

Compiled & Edited by
Pauline C. Reich

Volume 3

WEST®
A Thomson Reuters business

For Customer Assistance Call 1-800-328-4880

Mat #41260170

Table of Contents

III. LEGISLATION

IV. RULES AND REGULATIONS

CHAPTER 14. INDUSTRY CASE STUDIES

CHAPTER 15. JUDICIAL CASES AND INDICTMENTS

A. UNITED STATES

1. INTERNET GAMBLING

2. CHILD PORNOGRAPHY

3. HACKING/NATIONAL SECURITY

4. DOWNLOADING/PEER-TO-PEER

5. SPAM

6. ONLINE PAYMENTS

7. SOLICITATION OF MINORS

Summary of Contents

Volume 1

Volume 2

Volume 3

Chapter 11

National Legislation and Commentary—Middle Eastern Countries

§ 11:1 Saudi Arabia: The Cyber Threat Landscape of Saudi Arabia; VeriSigniDefense Global Threat Research Report

The Cyber Threat Landscape of Saudi Arabia

Nov. 28, 2008*

Table of Contents

[Section 11:1]

*Reproduced with the permission of VeriSign, Inc.; © 2008 VeriSign, Inc.

The Cyber Threat Landscape of Saudi Arabia

Nov. 28, 2008

1 Executive Summary

Saudi Arabia is geographically the largest country in the Arab world. It is also, unquestionably, the most significant country not only in the Arab world but also in the entire Islamic world, given that its

territory includes the two holiest shrines of Islam, which are located in Mecca and Medina. Aside from this, the country's huge petroleum wealth has also made Saudi Arabia an important center of business in the Middle East. Internet censorship notwithstanding, Saudi Arabia also has a very substantial Internet and telecommunications infrastructure, which the country's business environment uses widely. This infrastructure has given rise to a relatively extensive indigenous hacker community. These facts, combined with the geopolitical circumstances and many other idiosyncrasies, make Saudi Arabia a challenging but potentially rewarding place to do business. After first providing an overview of the telecommunications and information technology (IT) environment, the IT and IT security-related aspects of the Saudi legal system, and an overview of the socio-political situation from an IT security perspective, this report will explore some aspects of doing business in Saudi Arabia, especially from regulatory, Cybercrime and cyber security points of view.

2 Threat Matrix Section

As this year comes to a close, iDefense analysts assess the threat levels for various cyber threats in Saudi Arabia as shown in Exhibit 2-1:

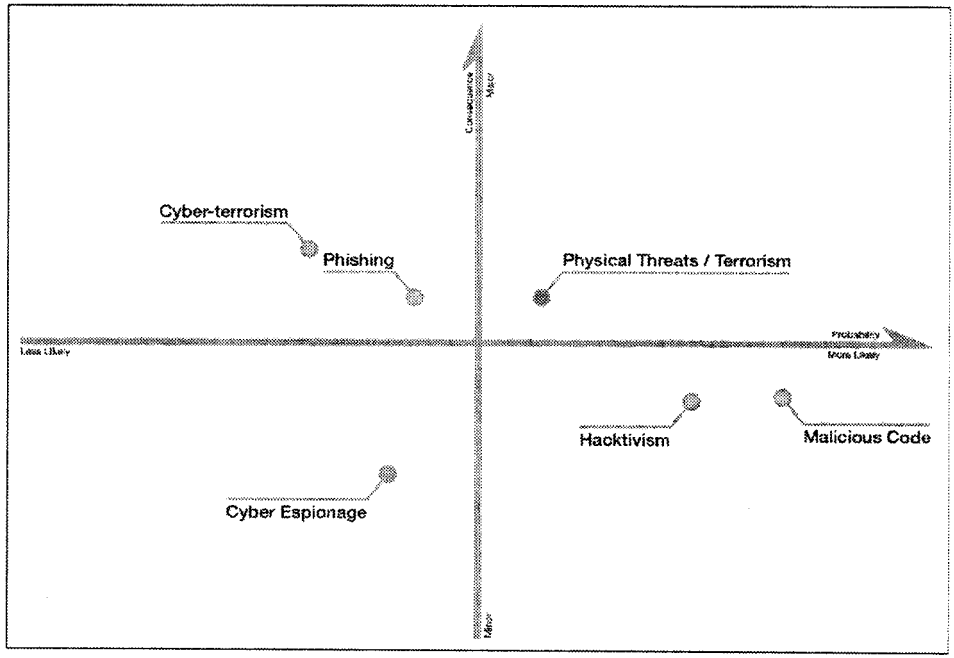

Exhibit 2-1: Overall Estimate of Cyber Threat Levels in Saudi Arabia

The exact level of risk for each type of threat will vary somewhat depending on number of related factors, such as connectivity to the

Internet, location in Saudi Arabia, the degree of publicity surrounding the business activities of a given company, and any political affiliations that the company or its business interests may carry with it. Bearing this in mind, the categories below are the kinds of cyber threats most likely to occur in Saudi Arabia:

1. Physical Threats and Terrorism: As previously indicated, Saudi Arabia's location, at the heart of the troubled Middle East region, necessarily entails a high risk of physical threat occurrence.

2. Hacktivism/Defacement Attacks: Hacktivism is a staple component of hacking in the Middle East. There is, perhaps, nowhere else among the world's hackers where ideologies and political conflicts have so much influence on what local hackers do. Most hacktivism takes the form of website defacements, which typically amount to no more than a relatively minor nuisance. For their part, some Middle Eastern hacker groups outside Saudi Arabia, such as in Turkey, are renowned for the ornate graphics of their defacements.

3. Cyber Terrorism: Cyber terrorism is defined here as a highly disruptive cyber attack, such as a distributed denial of service, infiltration of servers, massive deletion of data content and other similar e-attacks that could seriously hamper the operations of a business. At their current average stage of proficiency, indigenous cyber terrorists are unlikely to possess the skills to carry out such attacks successfully. Hence, the probability of cyber terror attacks is rather low; however, if they do occur, the consequences to business operations from such attacks could be major.

4. Cyber Espionage: This threat category relates to the telecommunications privacy laws and rights touched on later in this report. Generally, the risks of cyber espionage are relative and very much depend on the nature of the business operation being conducted. A bank, for instance, is not very likely to invite the scrutiny of government-sponsored cyber espionage campaigns. The bank, however, might invite such scrutiny if suspected terrorists were doing business with it. Meanwhile, if the business operation were to, in some way, be involved with local dissidents or otherwise engagage in activities that the government finds objectionable—however tenuous the connection may be the chances of cyber espionage could increase dramatically.

5. Phishing and Malicious Code Attacks: There is at present a moderate level of risk for phishing and malicious code attacks, especially since the number of indigenous phishing and malicious code hackers is low compared to those of Russia or China. This is especially because traditional criminal motives, such as financial gain, are not the main motivation for Saudi hackers, at least compared to ideology and political issues.

3 Saudi Arabia Telecommunications and IT Infrastructure

The history of telecommunications services in Saudi Arabia began

with the reign of the country's King Abdul-Aziz in 1930. During this reign, the first telephone exchange was installed in Al-Dira, an area within Riyadh. In 1953, the country's Ministry of Communications was established to handle postage and telecommunications affairs. Within a year after the Ministry had first been formed, the Saudi Arabian Radio Telecommunication system, RT-1, was established to provide a multi-channel telephone and telegraph network between the cities of Riyadh, Dammam, Makkah, Medina and Al-Ta'if. In 1977, the Ministry of Post, Telegraphs and Telephones, which had earlier taken over the telecommunications responsibilities from the Ministry of Communications, began a project to set up a modern telecommunications network in the country, with telephone, telegraph and telex services.[1]

In May 1998, Saudi Arabia's telecommunications services privatized, an action that gave rise to the Saudi Telecommunications Company (STC). The STC soon became one of the largest employers in the kingdom, with jobs for more than 70,000 Saudi citizens. In May 2003, the Ministry of Post, Telegraphs and Telephones was renamed the Ministry of Telecommunications and Information Technology, a title it carries to this day. As of the end of 2006, the number of fixed telephone lines in the country exceeded four million, three million of which were household telephone lines.[2] Meanwhile, the mobile phone sector is experiencing phenomenal growth, with the number of mobile users estimated to be more than 20 million as of this writing.

3.1 General Regulatory and Oversight Environment

The principal organizations behind the telecommunications and IT environment of Saudi Arabia are as follows:

A. The Ministry of Communications and Information Technology (MCIT)

His Eminence Mohammed Jamil Bin Ahmad Mulla currently heads the Saudi MCIT, which is the main authority of reference in all communications and IT affairs in Saudi Arabia, [www.mcit.gov.sa.]

B. The King Abdullah City of Science and Technology (KACST)

With headquarters in Riyadh, the KACST is a well-known Saudi government scientific institution, [www.mcit.gov.sa], established to support and foster scientific research and development in Saudi Arabia in various fields, and IT-related research figures among these fields. Consequently, the KACST operates many major IT infrastructure components in Saudi Arabia, and national IT-related projects are sure to involve major participation by this institution in any number of advisory or applied capacities. In administrative

[1]http://www.saudinf.com/main/g51.htm

[2]https://www.cia.gov/library/publications/the-world-factbook/geos/sa.html

terms, it is subordinate to the chairperson of the Saudi Council of Ministers.[3]

C. The Communications and Information Technology Commission (CITC)

Working closely with the Ministry of Communications and Information Technology, the Saudi Arabia CITC describes its main goal in its mission statement: "universally available, high-quality portable communications and information technology services." In providing these services, it plays a major part in establishing the regulatory framework governing telecommunications and IT services in Saudi Arabia, [www.mcit.gov.sa][4]

D. The Saudi Computer Society

The Saudi Computer Society, formed in 1988, was the first nonprofit national institution concerned with activities in research involving scientific and cultural progress in computer science and IT, [www.mcit.gov.sa]. It organizes conferences, seminars and exhibits in different computer-related fields in an effort to attract various types of IT specialist to collaborate for the greater benefit of the country.[5]

3.1.1 CERT Operation and History

Many countries of the world have a regional Computer Emergency Response Team (CERT); Saudi Arabia is no exception, [www.mcit.gov.sa]. CERT of Saudi Arabia (CERT-SA) is like the Internet itself in Saudi Arabia, a relatively recent phenomenon. Currently, CERT-SA is in what it refers to as "phase II" of its implementation, with the first phase having been completed in 2007. Phase II involves "incremental operation and capacity building, and a strategy of monitoring, response, and coordination." Meanwhile, the final stage of its establishment, phase III, is expected to be implemented in 2009.

Like its sister organizations in other countries, the objective of CERT is to foster a greater level of IT security awareness in Saudi Arabia through dissemination of IT security knowledge, availability of education and training, dissemination of important IT security-related announcements, alerts and warnings, IT security incident support, and related analysis. The organization also aims to function as a reference point and authority in information security for Saudi Arabia's community of IT security professionals and other computer users. It additionally aims to help foster the skills and knowledge to effectively

---

[3]http://www.kacst.edu.sa/ar/aboutkacst/pages/main.aspx

[4]http://www.citc.gov.sa/citcportal/SimpleText/tabid/103/cmspid/%7BD2108899-41DC-4-C4E-BD69-F49E36FB421A%7D/Default.aspx

[5]http://www.computer.org.sa/About_SCS.asp

deal with information security issues in the kingdom among Saudi citizens.[6]

3.1.1.1 Comparison to US or Relevant Regional CERT

As a newly founded organization that had not completed its establishment in Saudi Arabia as of this writing, the CERT-SA is still a fledgling organization compared to other CERT organizations, such as those in the US or Europe. With a welldeveloped website, mailing lists for members and an actively functioning distribution of IT security-related news feeds, its prominence and utility in the local IT security community is likely to grow, especially as Internet use and IT security issues become more prominent in Saudi Arabia.

3.1.2 Internet Privacy, Data Protection Laws, Use of Encryption and Related Legal Issues

On the subject of Internet privacy and data protection, the following English version of Chapter 8 from Saudi Arabia's Telecom Bylaw entitled "Relations between Service Providers and Users" provides some very important insights. Underlined text denotes particular clauses that delineate limits to privacy rights:[7]

---

[6]http://www.cert.gov.sa/index.php?option=com_content&task=blogsection&id=18&Itemid=109

[7]http://www.citc.gov.sa/citcportal/CommissionStatutesDetails/tabid/113/cmspid/%7BA4FF3A7C-E8D2-41A9-BC6F-7C26F06C9D11%7D/Default.aspx