P. O. Box 9170, Riyadh 11423
Kingdom of Saudi Arabia
Tel. +(966-11) 462-5925

Mohamed Al-Sharif
License No. 96/26

THE LAW FIRM OF
MOHAMED AL-SHARIF

IN ASSOCIATION WITH
JOHNSON & PUMP

chris@alshariflaw.com

Saudi Arabia Cybersecurity: Issues During COVID-19

Given the widespread use of remote working, there is a growing risk of cyberattacks.Attacks can take the form of requesting company details (phishing), malware to monitor web use and obtain sensitive data such as passwords and digital assets, and programs that threaten to wipe data or disclose personal information if a ransom is not paid (ransomware). Recent state-sponsored attacks have targeted Saudi agencies and companies (https://reut.rs/3bnsTPV), and non-state actors seek to exploit vulnerabilities for financial gain. Companies in the defense, utilities, energy, health and e-commerce industries are at particular risk.

To illustrate the risk, an employee might receive an email that appears to come from a supervisor with an attachment labelled “work from home policy.” When opened, the attachment launches a virus that extracts company emails from the laptop.

Here some key reminders for your employees to minimize the risk:

1. **Implement procedures for handling sensitive information:** Attacks often target corporate data and other digital assets. Employees should be instructed to follow safe procedures when handling such assets remotely. Avoid using personal email addresses and personal computers and do not open suspect messages. Ensure anti-malware software is installed on all computers.
2. **Use a secure network**: Attacks targeting a network can intercept information and gain access to connected computers. Ensure network software, passwords, and permissions are up to date.
3. **Take caution when printing at home**: Printers can also be targets of cyberattacks. If the printed document would be subject to shredding in the office environment, take care to segregate and shred that same document at home.

Saudi Arabia has a dedicated government body, the National Cybersecurity Authority, which provides specific guidance https://nca.gov.sa/en/index.html. Applicable laws depend on the type of company and its business. Major legislation and guidelines include:

- The Anti-Cybercrime Law: https://bit.ly/3bjU5im

- The Controls of the Use of Computers and Information Networks in Government Entities: https://bit.ly/3drwRJ9
- Essential Cybersecurity Controls (ECC – 1 : 2018): https://bit.ly/2wo2SBe
- The National Information Security Strategy (NISS): https://bit.ly/2UhRArn
- Resolution No. 555 of 2019: https://bit.ly/2UxUxms
- Royal Order 57231 dated 10/11/1439 H
- SAMA's Cyber Security Framework (applicable for the banking sector): https://bit.ly/2J9jKyd

Given the ripe opportunities for cyberattacks, this is an appropriate time for companies to implement or update organizational policies on digital assets and services, confidentiality, codes of conduct, and business ethics.

We will be happy to schedule a consultation, either in person or remotely, where we can provide more specific advice after a review of your contracts and a better understanding of your particular circumstances, concerns, and priorities.