


Chapter 96

Critical Cybersecurity Threats: Frontline Issues Faced by Bahraini Organizations

Adel Ismail Al-Alawi

 <https://orcid.org/0000-0003-0775-4406>
University of Bahrain, Bahrain

Sara Abdulrahman Al-Bassam

 <https://orcid.org/0000-0003-0094-6149>

The Social Development Office of His Highness the Prime Minister's Diwan, Kuwait

Arpita A. Mehrotra

Royal University for Women, Bahrain

ABSTRACT

One common reason for cybercrime is the goal of damaging a business by hacking or destroying important information. Another such reason is the criminal's goal of gaining financially from the hack. This chapter analyzes Bahraini organizations' vulnerability to digital security threats. It has used qualitative research to analyze industry performance. Moreover, with the support of secondary research, it has also explored cybersecurity threats faced by such organizations. The discussion based on secondary data analysis has explored two major aspects of Bahraini organizations and the cybersecurity threats they face. Firstly, the data and finances of both sectors are at huge risk in Bahraini organizations. Secondly, one important aspect of exploration has been to identify the most frequently encountered forms of cybercrime. Its analysis reveals that the kind of cybersecurity threat that a business is most likely to face is cyberwarfare. This may affect two rival businesses while they are competing with each other. Competitors' data may be destroyed or hacked—leading to long-term losses.

DOI: 10.4018/978-1-7998-8954-0.ch096

INTRODUCTION

Continuous improvement in organizational processes adheres to the principle of technological development. Constant progress usually involves technological development. Reasons include customizing work-related processes, optimizing workflow efficiency to improve turnaround time, and improving performance (Elmaghraby & Losavio, 2014). However, an increase in technological development may result in business data being stored in the cloud or on at-risk devices—making such data vulnerable to emergent threats (Abawajy, 2014).

Hence, cybersecurity issues have emerged in response to technological advancement. This chapter report intends to analyze present-day cybersecurity issues in industries and their impact on organizations. Information technology has become inseparable from all daily activities and is in the process of becoming a civilizational-structuring factor. However, vulnerabilities in digital infrastructure hardware and services, as well as the characteristics of the Internet itself, favor the expression of crime and of expanded opportunities for criminal malfeasance. The present day has witnessed the rise of cybercrime incidents affecting everyone (to varying degrees). Al-Alawi and Abdelgadir (2006) stated: “Computer crime has emerged as one of the major forms of sabotage[—]causing millions of dollars’ worth of damage annually. These attacks usually come in the form of viruses, worms, denial of service attacks, and hacking.” Whether it is gross incivility, harassment, fraud, theft, destruction, malfunctioning, surveillance, spying, hacktivism, terrorism, or deliberate misinformation—or any form of crime—violence and conflict is drawn to the Internet like a moth to flame. Understanding the risks to which the individual, the public and private organization, the state, and (more generally) society faces such threats enables us to act in informed ways. In order not to remain destitute and passive in the light of problems caused by cyber-attacks or the misuse of technology, political and economic stakeholders must take ownership of the fundamentals of cybersecurity necessary for the control of risks and the harmonious development of the digital ecosystem. Any pragmatic response to security, protection, disaster mitigation, and emergency response needs to be generated by the digital world. Our interactions and our dependence on information systems, cyberspace, and the Internet, need to be based on a strategic approach which sets the framework for taking action. This strategic vision is needed to govern, steer, and ensure the coherence and complementarity of strategic and operational measures. This also allows for efficiency and effectiveness (Emirates 24/7, 2014).

Examining the roles and risks of technology is prudent in every type of organization. Military, governmental, private, and nonprofit organizations use different forms of hardware; software; the Internet of Things (IoT); cloud data; and other technologies (Cavelty, 2014). According to Emirates (2014), security in the form of cybersecurity and physical security is required. As is supported by Brookes (2015), sensitive information is presented in different technological formats in the organizations—a fact which has always required an appropriate cybersecurity system. The emerging trends of cyber hacking may put organizations into a state of threat (Joiner, 2017). The discussion on the topic is essential for providing managerial-level implications and recommendations. The *desk research method* used in this chapter basically consists of collecting data from a variety of efficient resources. The secondary analysis can reinforce researchers’ commitment to strengthening their knowledge base in given areas of research. Heaton (1998) stated, “Secondary analysis involves the utilization of existing data, collected for the purposes of a prior study, in order to pursue a research interest which is distinct from that of the original work.”

Secondary research of the security issues of Bahraini organizations has been undertaken with respect to qualitative research. For this purpose, secondary data on the Bahraini security threats have been ana-

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/critical-cybersecurity-threats/280266

Related Content

Computational Complexity Analysis for a Class of Symmetric Cryptosystems Using Simple Arithmetic Operations and Memory Access Time

Walid Y. Zibidehand Mustafa M. Matalgah (2013). *International Journal of Information Security and Privacy* (pp. 63-75).

www.irma-international.org/article/computational-complexity-analysis-class-symmetric/78530

An Analysis of Economic Growth for Major Advanced Economies

Hakan Altin (2022). *International Journal of Risk and Contingency Management* (pp. 1-22).

www.irma-international.org/article/an-analysis-of-economic-growth-for-major-advanced-economies/295958

Malware: An Evolving Threat

Steven Furnelland Jeremy Ward (2008). *Security and Software for Cybercafes* (pp. 147-169).

www.irma-international.org/chapter/malware-evolving-threat/28535

Watermarking for Still Images Using a Computation of the Watermark Weighting Factor and the Human Visual System in the DCT Domain

O-Hyung Kwonand Rae-Hong Park (2013). *Multimedia Information Hiding Technologies and Methodologies for Controlling Data* (pp. 286-304).

www.irma-international.org/chapter/watermarking-still-images-using-computation/70293

A Comparative Analysis of Chain-Based Access Control and Role-Based Access Control in the Healthcare Domain

Esraa Omran, Tyrone Grandison, David Nelsonand Albert Bokma (2013). *International Journal of Information Security and Privacy* (pp. 36-52).

www.irma-international.org/article/a-comparative-analysis-of-chain-based-access-control-and-role-based-access-control-in-the-healthcare-domain/95141