Chapter 20
Digital Security Strategy

ABSTRACT

This chapter analyzes digital security strategies for the 21st century. The chapter begins by examining different types of cyberattacks, such as identity theft, malware, and phishing. Next, the chapter reviews statistics about cyberattacks in the US and the world, focusing on the monetary costs. The typical targets of cyberattacks are then considered, followed by a discussion about how to prevent cybercrime. The chapter next reviews digital security indicators that can provide valuable information about cybercrime and cyberattacks. After this, the chapter discusses cyberwar, which involves cyberattacks not just used against individuals and companies, but against entire states. The chapter concludes by advancing a digital security strategy that can be used in the 21st century.

INTRODUCTION

A cyberattack is an attack carried out from one or more computers against another computer(s) or a computer network. Cyberattacks can be divided into two general types: (a) attacks designed to disable the target computer or take it offline, and (b) attacks that aim to gain access to the data of the target computer or gain administrator privileges.

Data breaches and digital security incidents are becoming increasingly costly. Desjardins Group, a Canadian lender, revealed that it spent $53 million as a result of a disclosure of 2.9 million of its members. In addition, the manufacturer Norsk Hydro reported that a recent cyberattack could cost them as much as $75 million. Finally, British Airways and Marriott, in addition to the costs of recent cyberattacks, had to pay $100 million each for failing to comply with the General Data Protection Regulation (GDPR) (Swinhoe, 2020).[1]

DOI: 10.4018/978-1-7998-8036-3.ch020

TYPES OF CYBERATTACKS

To achieve the goal of accessing or disabling computer networks, cybercriminals use several different technical methods. New methods are always being developed, and some categories overlap, but the following are some of the most popular:

- **Identity theft** is also one of the worst-case scenarios that can meet a victim of cybercrime. It starts with someone stealing another's identity by using identifiable data, such as victim's name, driver's license, and social security number. The thief then commits fraud, steals property, embezzles goods or uses services in the victim's name.
- **Cyberbullying** is when person tries to intimidate or harass others using computer systems connected to the Internet. Most cases of cyberbullying involve the use of communication systems such as email, social networks, and instant messaging, which allows the cyberbully to keep their identity anonymous.
- **Social engineering** is one of the most classic types of cyberattacks that can be carried out against individuals or organizations. It involves manipulating people to obtain valuable information that can later be used to illegally log into privately protected systems or networks. Often, the primary motivation behind social engineering is the theft of money, financial data (such as bank accounts or credit card information), and other confidential information from a company or customer.
- **Botnets** are cyberattacks that involve the use of one or more bots connected over a network (e.g., the Internet). The word "botnet" comes from blending the words "robot" and "network". These botnets are used to spread malicious files and software, infect other systems, carry out Distributed Denial-of-Service (DDoS) attacks, steal data, and send spam messages.
- **Malware** refers to any software, regardless of its structure or operation, which is designed to damage a single computer, server, or computer network. Worms, viruses, and Trojans are variations of malware that differ in the way they multiply and spread. These attacks can cause a computer or network to stop working or give an attacker root access to control the system remotely.
- **Phishing** is a technique in which cybercriminals produce emails to deceive a target and take malicious actions. The recipient may be tricked into downloading malware that is hidden in a valid document, or they may be asked to click on a link to a fake website where they will be asked to provide sensitive information, such as bank usernames and passwords. Many phishing emails cast a wide net and are sent by email to thousands of potential victims, but some are designed explicitly for valuable targets to try to convince them to share useful information.
- **Ransomware** is a variant of malware that encrypts the victim's files. The attacker then demands a ransom from the victim to restore access to the data after payment. Users are shown instructions on how to pay for obtaining a decryption key. The costs can range from a few hundred dollars to thousands and are usually paid to cybercriminals in cryptocurrencies.
- **Denial of service** is a method of brutal force, which involves preventing the proper functioning of some online services. For example, attackers can send so much traffic to a website or so many requests to a database that it overwhelms the ability of these systems to operate, making them inaccessible to anyone. Distributed Denial-of-Service (DDoS) attacks use an army of computers, usually compromised by malware and under the control of cybercriminals, to direct traffic towards targets.