Information Security Audit Program

Keith M. Hall

College of Science and Technology, Bellevue University

CYBR615-T302: Cybersecurity Governance

Professor Erich Krueger

August 06, 2023

Information Security Audit Program

A cyberattack has the potential to disrupt an entire industry, destroying any vulnerable business in its wake. In 2023, the global average cost of a single data breach was $4.45 million, a 15% rise in just 3 years (Cost of a Data Breach 2023 | IBM, n.d.). But despite the term's widespread use, there is still no consensus on what a cyberattack is (Hathaway et al., 2012; Roscini, 2014), and a recent finding showed that only 50.17% of organizations thought they were fully prepared for an attack (Gregory, 2022). Most information security issues are currently being handled by security tools and technology like encryption, firewalls, and access management. Although tools and technology should unquestionably play a crucial role in an organization's information security strategy, the literature suggests that they are insufficient on their own (Otero, 2019). This study investigates the cyberattacks perpetrated against Marriott International and Magellan Health in 2020 and reviews recent findings to pinpoint the security audit controls and procedures that would have helped lessen the impact of these assaults had they been in place.

What is A Cyberattack

Before going into the details of the cyberattacks, it is important to clarify what is meant by the term and gain some background knowledge about the organizations that were targeted. Doing so will provide context and help identify the crucial elements that led to the attacks. Only then can we identify the appropriate audit controls that were required to prevent or lessen the impact of the attacks.

The definition of a cyberattack varies considerably. In an article published in Technology Innovation Management Review, Mehdi Kadivar (2014) proposed an approach that can be used to construct a more complete definition. Kadivar devised a list of characteristics of a cyberattack by comparing definitions found in the literature and identifying the similarities in 10 high-profile cases. Each of these characteristics was seen in the current investigation. Using Kadivar's approach, a cyberattack can be defined as any attempt by a threat actor to gain unauthorized access to, interfere with, hinder, degrade, or destroy information system assets or the information itself for a covert purpose or immediate, concrete gain. This definition alludes to the reality that many cyberattacks go unnoticed. The motive behind a cyberattack can be "passive" or "active," with the former involving merely watching or listening in on a system or network and the latter entails taking direct action to harm or gain control of an asset (Otero, 2019). Organizations need to be aware of the existence of both types.

Marriot International

Marriott International Inc (Marriott) is a hospitality services provider that primarily operates, leases, and licenses hotels, residences, and timeshare properties under a variety of luxury, premium, and select brand names such as the Ritz-Carlton and Westin Hotels. Marriott provides lodging, hotel reservations, timeshare vacations, airfare and hotel packages, and car rental. It also runs reward programs such as Marriott Bonvoy. (Marriott International Inc Company Profile - Marriott International Inc Overview, n.d.).

The Cyberattack (2020)

The popular hotel operator experienced a data breach in 2020. Using the login information of two employees who worked at a franchise facility, threat actors gained access to 5.2 million hotel guests' records. An application used by all Marriott properties to deliver guest services was the target of the attack and seems to have been the work of a lone individual. Marriott stated that it had no reason to suspect that the guest services information included Marriott Bonvoy account passwords or PINs, payment card information, passport information, national IDs, or driver's license numbers. However, the hacked data may have included contact information and information linked to customer loyalty accounts, but not passwords (Marriott Discloses Data Breach Affecting Around 5.2 Million Guests, 2020).

Magellan Health

The healthcare provider Magellan Health focuses on providing benefits for mental health. To give members access to therapeutic services from a wide provider network, many health insurance companies collaborate with Magellan. As a result, many of its members obtain mental health services from Magellan Health even if they have health insurance plans with other insurance providers. The business offers its solutions to different military and governmental institutions, labor unions, employers, third party administrators, managed care organizations, and others (Magellan Health | Mental Health Coverage | ZenCare, n.d.).

The Cyberattack (2020)

The attack involved data exporting and the deployment of ransomware using a social engineering phishing scheme. To access the targeted system, malicious actors first acquired employee login information. Health insurance, treatment information, email addresses, phone numbers, physical addresses, and Social Security numbers were among the data stolen from patients and employees (Magellan Health | Mental Health Coverage | ZenCare, n.d.).

Audit Controls and Procedures

Security Audit Controls refer to the audit arrangements in place that ensure security controls and procedures are effective (Audit Control Definition | Law Insider, n.d.). In this section, we outline the audit controls and processes that would have helped to prevent or mitigate the consequences of these assaults. In the following section, we will explain briefly how.

The Marriott International and Magellan examples are similar. So much so that both assaults could have been carried out by the same threat actors. Both featured a network breach that was the direct result of two employees whose login credentials fell into the wrong hands. Marriott did not disclose how the hackers obtained employee credentials. Magellan, however, stated that phishing was used to obtain passwords. Despite these differences, the list of audit controls below is applicable in both instances.

- Assess whether password length and complexity support levels of security consistent with policies and/or best industry practices.
- Examine, record, and scan for vulnerabilities in the authentication processes.

- Evaluate the effectiveness of identity management and trust policies and practices, including encryption and access controls.
- Check the effectiveness of training policies and materials (Otero, 2019).

Results

1) By assessing whether password length and complexity support levels of security consistent with policies and/or best industry practices, auditors can help enforce adherence to them. This would have reduced the likelihood that weak or shared passwords were the cause of the breach. 2) A review of training policies, procedures, and materials relating to proper password management and how to avoid and report phishing attempts would have helped thwart a successful phishing attack and revealed whether any changes were required. It is commonly accepted that the human aspect is typically the weakest link when it comes to IT security. Most CIOs (Chief Information Officer) are supporting the implementation of security awareness programs to strengthen this link (P. Tarwireyi et al., 2011), 3) Evaluating identity management and trust policies and practices, including encryption and access controls is also critical. Identity management solutions are designed to protect the network should passwords be compromised (zero trust). Businesses that implement strict encryption rules and employ high-grade encryption can lessen the negative effects of data theft and leakage. But first, the effectiveness of the current controls would need to be continuously tested and evaluated. 4) As early as 2020, had auditors scanned and recorded vulnerabilities and examines authentication processes against standards, they would have suggested Marriott implement two factor authentication (Otero, 2019).

Although the damage was minimal in both examples, any unauthorized access to an organization's information assets is an eminent threat that must be addressed and mitigated. From the results of a review of the available literature about the breaches, it is likely that the audit controls identified in this study would have helped to avoid the attacks or ensure that the damage remained within acceptable levels of risk tolerance.

Reference List

Audit Control Definition | Law Insider. (n.d.). Law Insider. https://www.lawinsider.com/dictionary/audit-control

Cost of a data breach 2023 | IBM. (n.d.). https://www.ibm.com/reports/data-breach

CSRC Content Editor. (n.d.). Cyber Attack - Glossary | CSRC. https://csrc.nist.gov/glossary/term/Cyber_Attack

Gregory, J. (2022). Only half of small businesses are prepared for cyberattacks. Security Intelligence. https://securityintelligence.com/news/only-half-small-businesses-prepared-cyberattacks/

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. 2012. The Law of Cyber-Attack. California Law Review. 100(4): 817-885. http://www.californialawreview.org/articles/the-law-of-cyber-attack

Information Technology Control and Audit; Otero, A.; 5th ed.; CRC Press; 2019.

Kadivar, M. 2014. Cyber-Attack Attributes. Technology Innovation Management Review, 4(11): 22-27. http://doi.org/10.22215/timreview/846

Magellan Health | Mental Health Coverage | ZenCare. (n.d.). Magellan Health | Mental Health Coverage | Zencare. https://zencare.co/health-insurance/magellan-health

Marriott International Inc Company Profile - Marriott International Inc Overview. (n.d.). GlobalData. https://www.globaldata.com/company-profile/marriott-international-inc/#:~:text=Marriott%20International%20Inc%20(Marriott)%20is,premium%2C%20and%20select%20brand%20names.

Marriott Discloses Data Breach Affecting Around 5.2 Million Guests. (2020, March 31). Airguide Online, NA. https://link-gale-

com.ezproxy.bellevue.edu/apps/doc/A625654263/GBIB?u=nebraska_bell&sid=bookmark-GBIB&xid=b0925377

P. Tarwireyi, S. Flowerday and A. Bayaga, "Information security competence test with regards to password management," 2011 Information Security for South Africa, Johannesburg, South Africa, 2011, pp. 1-7, doi: 10.1109/ISSA.2011.6027524.

Roscini, M. 2014. Cyber Operations and the Use of Force in International Law. Oxford: Oxford University Press.

SecuLore. (n.d.). South Carolina - Cyber-Attack Archive | SecuLore. https://www.seculore.com/resources/cyber-attack-archive/south-carolina