UNIVERSITY OF HERTFORDSHIRE (UH)

SCHOOL OF PHYSICS, ENGINEERING AND COMPUTER SCIENCE

COURSE: MSc COMPUTER SCIENCE WITH CYBER SECURITY

MODULE: PENETRATION TESTING 7COM1068-0206-2023

ACADEMIC YEAR: 2023-2024

ASSIGNMENT TITLE: THREAT MODEL

NAME: OLUWATOBI ELIJAH AKANNI

STUDENT NUMBER: 22060310

Table of Contents

Table of Figures

ABSTRACT

T's Bank, a global financial institution with a diverse presence, faces cybersecurity risks due to its complex IT infrastructure and history of data breaches. This study utilizes an Attack Tree model to identify vulnerabilities and recommends prioritizing cybersecurity solutions to safeguard operations and client assets.

1.0.INTRODUCTION

In an era of global connectivity, cyber threats loom large for financial institutions like T’s Bank. With a complex IT infrastructure and a history of data breaches, the bank faces significant risks to its operations and client assets. Strengthening cybersecurity measures is crucial to protect against external and internal threats, ensuring the security of digital services and client information.

1.1. OVERVIEW OF THE ORGANIZATION

Global financial sector data breaches in (2023) were the second most costly behind healthcare. T’s Bank is a prominent financial services conglomerate that operates in a variety of countries, including Nigeria, Zambia, Kenya, The Gambia, Ghana, France, Cameroon, Mozambique, Botswana, Sierra Leone, South Africa, Rwanda, Guinea, United Kingdom, and the Democratic Republic of the Congo. The company also has branches in Lebanon, India, China, and the United Arab Emirates.

T's Bank, a worldwide banking organisation with a large customer base and a variety of financial goods and services, is vulnerable to cybersecurity threats owing to its activities in numerous jurisdictions with differing cybersecurity rules. The bank provides online banking and mobile applications, making it a prominent target for cyber-attacks.

Between July 2023 and the present day (2024), T’s Bank suffered data breaches that exposed client information such as Bank Verification Numbers (BVNs), names, addresses, and other sensitive information.

With a complicated IT architecture and a large amount of private financial data, T’s Bank is an appealing target for hackers, including both external threats from foreign actors and internal dangers from disgruntled employees. The bank's dependence on technology for day-to-day operations puts it exposed to interruptions caused by cyberattacks on its information technology systems

1.2. METHODOLOGY

The study provided in this paper is based on an Attack Tree model that shows numerous attack scenarios and vulnerabilities in T’s Bank systems. This strategy helps in discovering potential paths that attackers may use to undermine the organization's security. To mitigate these risks and continue operations.

T’s Bank must prioritise cybersecurity solutions that protect its systems and its clients' digital assets.

2.0. ATTACK TREE

Attack Trees provide a systematic approach to illustrating system security by mapping out various threats. A hierarchical structure is used to depict attacks on a system, with the main objective at the core and different methods of achieving it as the branches (Bruce, 1999).

These trees can be applied to analyze security issues in diverse domains such as oil/gas pipelines, chemical plants, information technology, infrastructure, and facilities. While Attack Trees are powerful tools for threat analysis, they may be overly complex when used to assess familiar scenarios like house break-ins, which are more straightforward and intuitive (Vineet, et al., 2008).

The practical application of Attack Trees has gained traction due to their user-friendly nature in threat analysis. However, the lack of precise semantics has led to ambiguity. Establishing a formal interpretation is deemed essential for a clear understanding of how Attack Trees can be effectively utilized in construction and analysis processes (Sjouke & Oostdijk, 2006).

The examination of Attack Trees at T's Bank revealed a range of significant cybersecurity threats, including external cyber-attacks, insider risks, physical security breaches, and vulnerabilities involving third-party vendors. These threats pose significant implications for the organization's operations, customer assets, and overall security posture

2.1. ATTACK TREE DIAGRAM

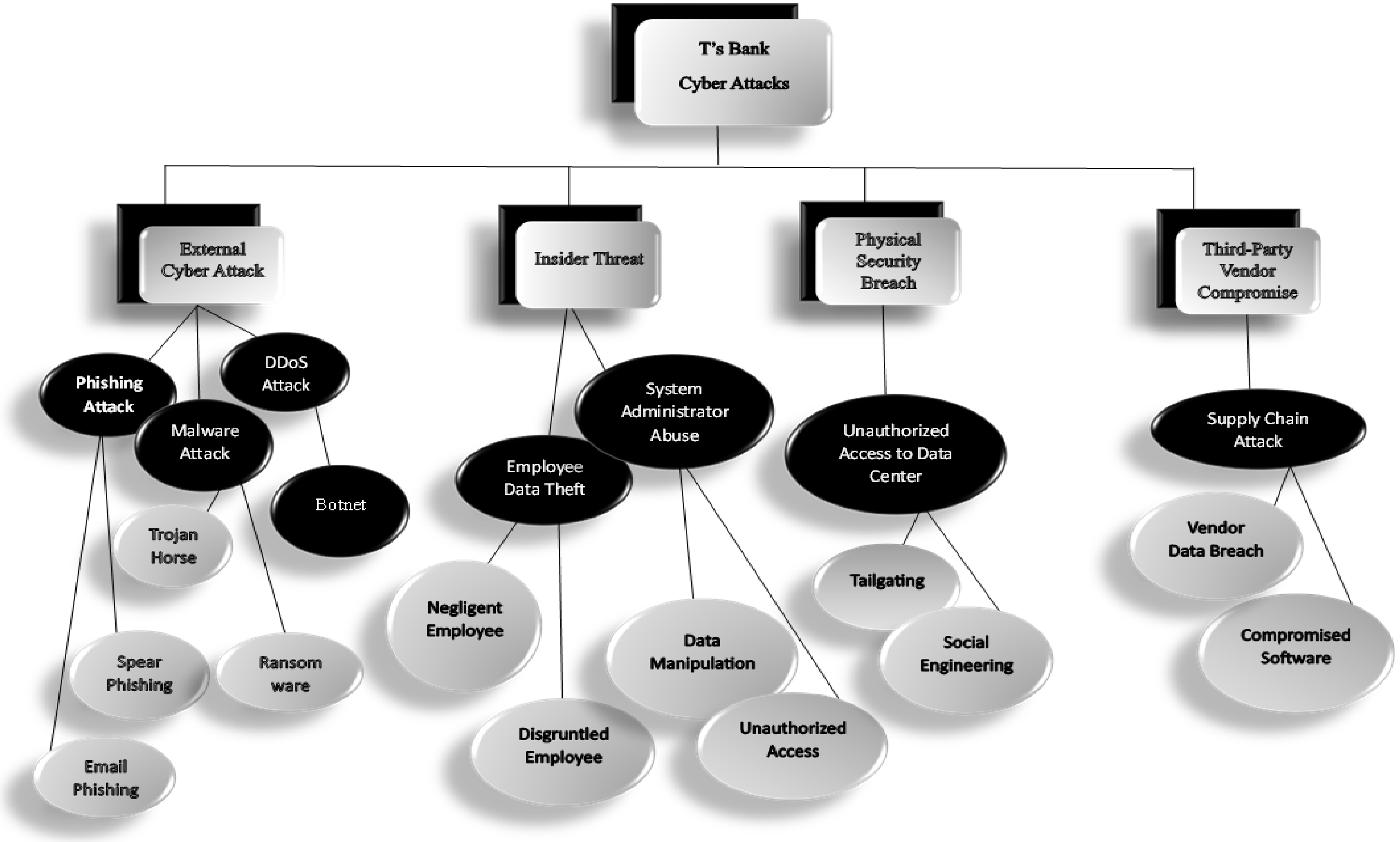

FIGURE 1: T's Bank Attack Tree Diagram

2.2. Findings and Discussion

According to research by ENISA threat landscape (2023), a significant 83% of cyber-attacks involved external actors, primarily organised crime groups driven by financial motives. However, internal actors played a notable role in 18% of cases, stemming from voluntary misuse or inadvertent errors.

Human error was a factor in 74% of breaches, with financial gain being the primary motivation in 95% of attacks, marking a 5% increase from the previous year. Espionage followed at around 5%. Notably, breaches involving cryptocurrencies quadrupled compared to the prior year. (Ifigeneia, et al., 2023)

Supply chain attacks outperformed malware-based breaches by 133%, affecting 10 million and 4.3 million victims, respectively. Data breaches involving insecure cloud databases dropped by 75%, while physical attacks fell to 46 incidents. System and human mistakes were steady compared to 2020, yet they still ranked third in terms of reported breaches.

This attack tree is important to T's Bank's threat profile because it considers the various ways the organisation might be targeted by cyberattacks, insider threats, physical security breaches, and third-party vendor compromises. These attack vectors correlate with the bank's features, such as its big client base, online services, sophisticated IT infrastructure, and reliance on technology, rendering it vulnerable to numerous types of cyber-attacks in the present threat landscape.

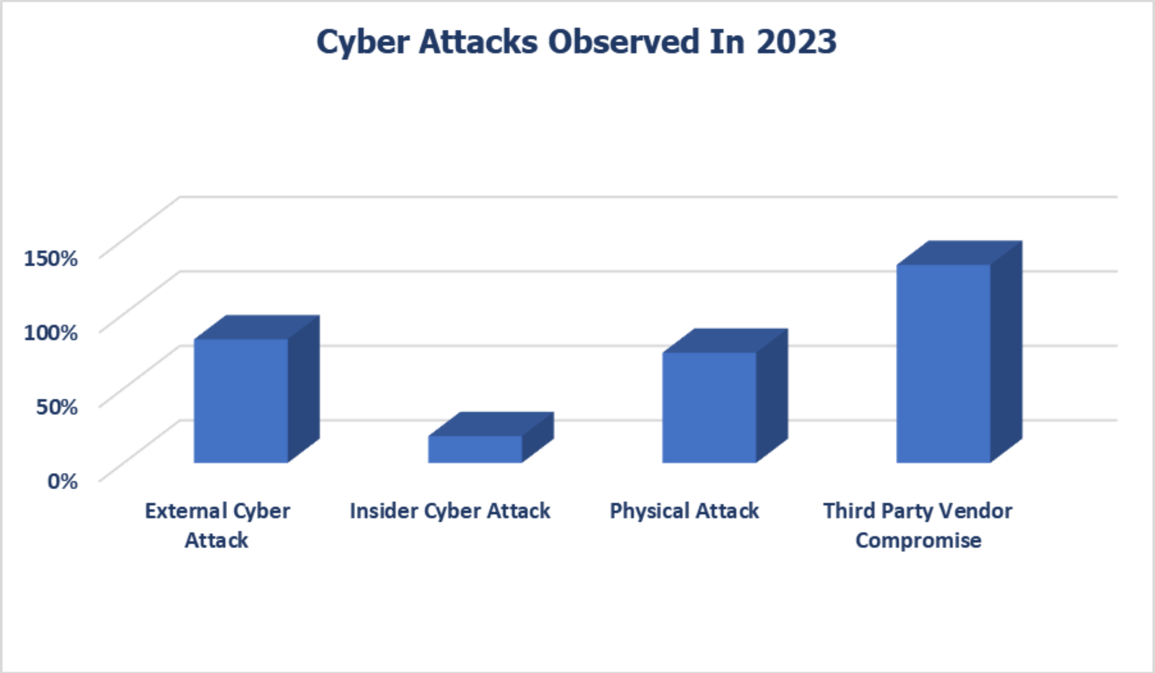

FIGURE 2: Cyber Attacks Observed In 2023

3.0. EVALUATION

3.1. SECURITY TECHNIQUES

T's Bank should improve its cybersecurity by implementing multi-factor authentication, offering security training, segmenting the network, using monitoring, and detecting systems, encrypting data, developing an incident response strategy, and conducting security audits. These activities improve security, educate employees, limit breaches, identify events, safeguard data, prepare for cyber threats, and resolve vulnerabilities.

3.2. METHODS, CONTROLS, AND PROCEDURE

To enhance cybersecurity, T's Bank should implement multi-factor authentication for all online and mobile banking transactions, conduct regular security audits and penetration testing, encrypt sensitive data at rest and in transit, enforce strict access controls, monitor network traffic for anomalies, and provide comprehensive cybersecurity training to all employees.

3.3. RECOMMENDATIONS

3.3.1. External cyber-attack:

PHISHING: T's Bank should deploy advanced email filtering technologies to intercept and block malicious emails before they reach employees' inboxes. Additionally, regular employee training sessions should be conducted to educate staff on how to recognize phishing attacks (Ömer, et al., 2023).

Malware: T’s bank should use robust antivirus software and endpoint detection and response solutions to detect and prevent malware infiltration. It is crucial to ensure that all systems and software are updated with the latest security patches to minimize vulnerabilities (Ömer, et al., 2023).

Distributed Denial of Service (DDoS): T's Bank should collaborate with a DDoS mitigation service provider to identify and neutralize large-scale assaults on its online services. Continuous monitoring of network traffic for unusual patterns can help detect and respond to potential DDoS attacks swiftly (Ömer, et al., 2023).

3.3.2. Insider threat:

Employee Data Theft: To mitigate the risk of employee data theft, T's Bank should implement role-based access control measures to restrict employees' access to sensitive data based on their job roles. Utilizing user activity monitoring technologies can help detect any suspicious behavior that may indicate data theft (Chirayath & S., 2023).

System Administrator Abuse: T’s bank should adopt Privileged Access Management (PAM) systems to manage and monitor privileged accounts, limiting unauthorized access by system administrators. Maintaining detailed audit trails and logs of system administrator activities can aid in quickly identifying any unauthorized actions (Chirayath & S., 2023).

3.3.3. Physical security breach:

T's Bank should implement Multi-Factor Authentication (MFA) for physical access control, allowing only authorized personnel to access the data center. Additionally, deploying security guards and CCTV surveillance at entrance points can help identify and deter unauthorized individuals attempting to gain access (Zhenhua, et al., 2023).

3.3.4. Third-party vendor compromise:

T’s bank should conduct thorough security evaluations before onboarding third-party vendors and regularly review their security policies. Encouraging suppliers to use secure coding practices and test their products before integration with the bank's systems (Hope, 2022).

REFERENCES

Bruce, S., 1999. Attack trees. *Dr. Dobb’s Journal 24,* Volume 12, pp. 21-29.

Chirayath & S., S., 2023. Insider Threats and Strategies to Manage Insider Risk. In: *In Human Reliability Programs in Industries of National Importance for Safety and Security.* s.l.:Singapore: Springer Nature Singapore, pp. 51-59.

Hope, B. E., 2022. *Five Common Shortcomings of Third-Party Management Programs in Financial Organizations and Recommended Risk Management Strategies,* Utica University: bronson2022five.

Ifigeneia, L. et al., 2023. *ENISA threat landscape 2023: July 2022 to June 2023,* s.l.: EU: European Union.

Moumita, D., Tao, X. & Cheng., J. C., 2021. BIM security: A critical review and recommendations using encryption strategy and blockchain. *Automation in construction,* Volume 126, p. 103682.

Ömer, A. et al., 2023. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics,* Volume 12, p. 1333.

Sjouke, M. & Oostdijk, M., 2006.. Foundations of attack trees. In: mauw2006foundations, ed. *Information Security and Cryptology-ICISC 2005: 8th International Conference, Seoul, December 1-2, 2005, Revised Selected Papers 8,.* Korea: Springer Berlin Heidelbe, pp. 186-198.

Vineet, S., Duan, Q. & Paruchuri, V., 2008. Threat modelling using attack trees. *Journal of Computing Sciences in Colleges,* Volume 23, pp. 124-131.

Zakaria, et al., 2019 . Feature extraction and selection method of cyber-attack and threat profiling in cybersecurity audit. In: zakaria2019feature, ed. *International Conference on Cybersecurity (ICoCSec).* s.l.:IEEE, pp. 1 - 6.

Zhenhua, Y. et al., 2023. A Survey on Cyber-Physical Systems Security. *IEEE Internet of Things Journal.*

Appendix

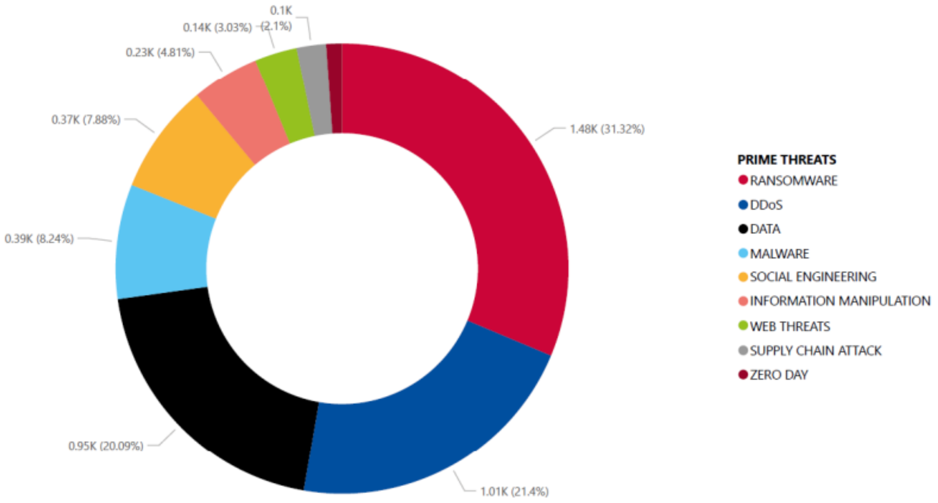

FIGURE 3: **Breakdown of analysed incidents by threat type (July 2022 till June 2023) (Ifigeneia, et al., 2023)**

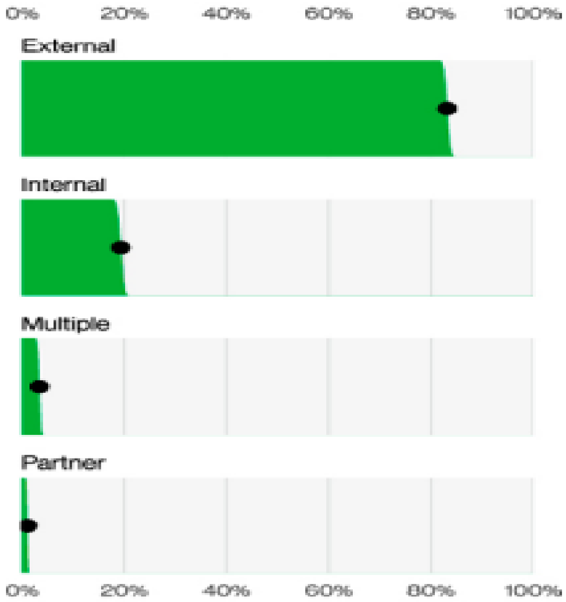

FIGURE 4: 2023 Data Breach Investigations Report (DBIR) (Verizon, 2023)

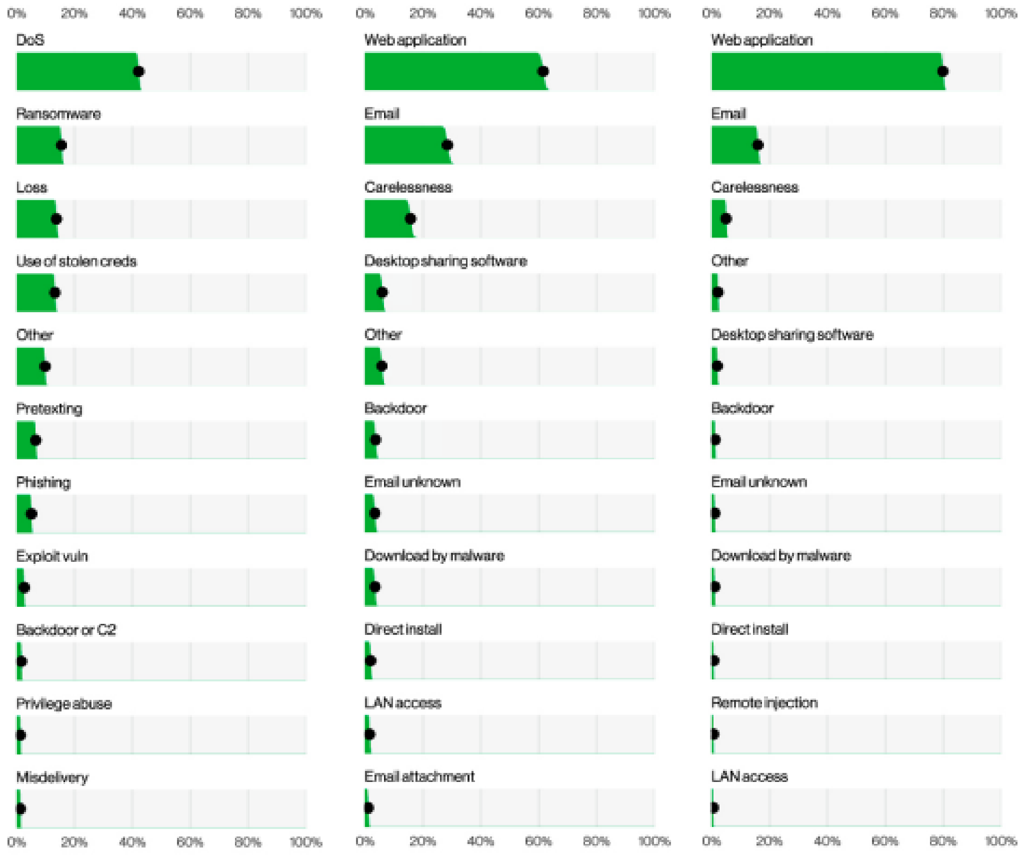

FIGURE 5: 2023 Data Breach Investigations Report (DBIR) (Verizon, 2023)