The new cloud security policy will be a positive step for the company, and it will be useful in the migration to the cloud. There are multiple risks and vulnerabilities that Burdell Bank needs to be aware of.

Threats & Risks

Social engineering poses a significant risk to Burdell Bank. Almost half of surveyed IT and security professionals had experienced at least 25 attacks in the preceding two years [1]. With each social engineering security incident costing victims $25,000 to $100,000, the prevalence and cost leads this to be a non-negligible risk to consider [2].

Insider threats attacks occur when a person who has authorized access to an organization's systems or data uses that to cause harm intentionally or unintentionally. The likelihood of these attacks is high. Insider threats can lead to the theft of sensitive data, disruption of operations, and compromised resources. Therefore, the impact of a successful insider attack is significant and potentially irreparable. Ultimately, insiders are a high-risk issue as 60% of data breaches are caused by insider threats [3].

Network attacks are common threats to cloud infrastructures with the potential to cause significant financial and reputational damage to the bank. Denial-of-Service attacks are a prevalent strategy amongst attackers. This attack uses a network of multiple devices or computers to flood an organization's network and servers causing services to become unavailable. According to the World Economic Forum, the average cost of a Denial-of-Service (DOS) cyber-attack is $1.1 million [4].

Misconfigurations are common vulnerabilities that the company could be facing, it is another example where human error accounts for a substantial proportion of these kinds of attacks. It is something the attackers are aware of which is why it happens to organizations more and more as well. Security misconfiguration occurs when system or application configuration settings are missing or are erroneously implemented, allowing unauthorized access. Common security misconfigurations can occur because of leaving default settings unchanged, erroneous configuration changes or other technical issues. According to research published in 2022 by IT auditing service provider Titania, network misconfigurations cost firms an average of 9 percent of annual revenue. However, the cost is likely to be higher [5]. They can occur in applications, cloud infrastructure, networks and elsewhere [6].

The new Cloud Security Policy for Banks is in line with the bank's mission and business model because it aims to implement secure cloud computing practices in the bank's IT infrastructure. The policy is based on the best practices and recommendations of the NIST Risk Management Framework SP 800-53. This is in line with the bank's goal of giving its customers reliable and safe financial services.

The Cloud Service Provider Requirements make sure that all cloud providers used by the bank's systems to access PII data follow the policy's minimum control standards. In line with the bank's commitment to data privacy and security, this makes sure that sensitive information about customers is always kept safe and cannot be transmitted or attacked by any outsider.

It shows that the bank is committed to providing a safe and compliant environment for its clients and stakeholders by making sure people follow the rules and punishing those who don't. Overall, the Cloud Security Policy is compatible with the bank's objective and business model, which is to provide dependable, secure financial services to consumers while guaranteeing regulatory compliance.

Compliance

This Cloud Policy for Banks shows a complete way to follow laws and other rules required. The policy is based on the **NIST Risk Management Framework SP 800-53**, which is a set of well-known best practices and security controls. Also, the policy's wide reach makes sure that all cloud-based services and systems in the bank's IT infrastructure, as well as all people who can use these systems, must follow the same strict rules. By doing this, the bank creates an environment that is consistent, safe, and meets legal and regulatory requirements.

Also, the policy makes it clear that all **regulatory requirements**, such as the FFIEC Guidelines, OCC Guidelines, FDIC Guidelines, GLBA, and PCI DSS, must be met. This approach makes sure that the bank follows the law and best practices while maintaining a strong and safe cloud computing infrastructure.

Our policy firmly follows NIST guidelines, ensuring that all actors with access to the bank's cloud resources and services are aware of any weaknesses and dangers the cloud infrastructure needs to cover up. We value NIST's identity, protect, detect, respond, and recover functions and follow them. We know there is no secret formula for cyber security within an organization, but the NIST standards that any organization can accept and use in their own ways depending on risk environment and business aim [7].

Recommendation

Since we have decided to migrate to the cloud, we need to invest sufficient resources into security for a successful transition from on-premises to the cloud. This transition to the cloud involves building a new infrastructure for the bank's data, so we should allocate resources to build a strong and secure foundation. Weak cloud security can lead to data breaches which results in losing money and losing customers' trust. The average cost of a data breach was $3.80 million for organizations with a hybrid cloud model and $4.24 million for those with private clouds [8]. Having an Incident Response (IR) team that regularly tests their plan can help organizations find cybersecurity weaknesses, strengthen their defenses, and save an average of $2.66 million in breach costs [8]. These breaches also result in customers being hesitant to use our bank which could lead to long term negative outcomes. By allocating sufficient resources, we can minimize the likelihood of a data breach which ultimately minimizes the risk. Thus, it is worth it to allocate resources now to build a secure cloud infrastructure to prevent data from reaching and losing trust.

References

[1] J. G. and S. Editor, "Social engineering attacks costly for business," CSO Online, 21-Sep-2011. [Online]. Available: https://www.csoonline.com/article/2129673/social-engineering-attacks-costly-for-business.html#:~:text=Social%20engineering%20attacks%20cost%20victims,security%20incident%2C%20the%20report%20states.&text=%5B%20Give%20your%20career%20a%20boost,Sign%20up%20for%20CSO%20newsletters.%20%5D. [Accessed: 15-Mar-2023].

[2] "Ilr.law.uiowa.edu." [Online]. Available: https://ilr.law.uiowa.edu/sites/ilr.law.uiowa.edu/files/2023-02/Pults.pdf. [Accessed: 09-Mar-2023].

[3] "Network attacks and network security threats," Cynet, 06-Jan-2023. [Online]. Available: https://www.cynet.com/network-attacks/network-attacks-and-network-security-threats/. [Accessed: 15-Mar-2023].

[4] "This is the crippling cost of cybercrime on Corporations," *World Economic Forum*. [Online]. Available: https://www.weforum.org/agenda/2019/11/cost-cybercrime-cybersecurity/. [Accessed: 15-Mar-2023].

[5] Reuters, "Treasury says cloud computing poses risks to financial sector," The Wall Street Journal, 08-Feb-2023. [Online]. Available: https://www.wsj.com/articles/treasury-warns-of-risks-to-financial-sector-in-cloud-computing-services-11675823799. [Accessed: 15-Mar-2023].

[6] "Security misconfiguration," Balbix, 19-Nov-2022. [Online]. Available: https://www.balbix.com/insights/security-misconfiguration-impact-examples-and-prevention/#:~:text=The%20impact%20of%20security%20misconfigurations,reputational%20damage%20to%20your%20organization. [Accessed: 15-Mar-2023].

[7] A. Mahn, "Identify, protect, detect, respond and recover: The NIST Cybersecurity Framework," NIST, 29-Nov-2022. [Online]. Available: https://www.nist.gov/blogs/taking-measure/identify-protect-detect-respond-and-recover-nist-cybersecurity-framework#:~:text=The%20Framework%20is%20risk%2Dbased%2C%20so%20it%20allows%20organizations%20to%20determine%20the%20appropriate%20level%20of%20cybersecurity%20for%20their%20individual%20risk%20environment%2C%20requirements%20and%20business%20objectives. [Accessed: 15-Mar-2023].

[8] "Cost of a data breach 2022," *IBM*. [Online]. Available: https://www.ibm.com/reports/data-breach. [Accessed: 15-Mar-2023].