International Journal for Research Trends in Social Science & Humanities
Volume 4, Issue 3
May-Jun- 2026, PP 1-6

A Study on Supply Chain Attacks as a Hidden Risk in Financial Software Used for Budgeting with Special Reference to Coimbatore City

Ms. Sakthi C[1], Ms. Rithika S[2], Mrs. Jeya Padma Deepa I[3]
[1,2]B. Com Corporate Secretaryship, Department of Commerce, Rathinam College of Arts and Science, Coimbatore.
[3]Assistant Professor, Department of Commerce, Rathinam College of Arts and Science (Autonomous), Coimbatore, Tamil Nadu.

Abstract: In the digital age, financial budgeting software has become an essential tool for individuals and organizations to manage finances, plan expenses, and support effective decision-making. Despite its advantages, the increasing reliance on such software has introduced significant cyber security concerns, particularly in the form of supply chain attacks. These attacks occur when cybercriminals exploit weaknesses in third-party vendors, external libraries, or software updates to gain unauthorized access to systems. As these elements are generally trusted, such threats often remain undetected until serious damage occurs. This study focuses on examining supply chain attacks as a hidden risk in financial software used for budgeting, with special reference to Coimbatore city. The research is based on secondary data, case studies, and insights gathered from financial professionals to understand the nature of these threats and the vulnerabilities involved. The study highlights the importance of adopting strong cyber security practices, including proper vendor evaluation, regular monitoring, and user awareness. It aims to provide practical suggestions to improve the security and reliability of financial software systems.

Keywords: Financial budgeting software, Supply chain threats, Cyber security challenges, Third-party risk, Software security, Data breach prevention, Risk assessment, Coimbatore region, Information protection, Cyber risk management.

I. Introduction:

In the modern digital environment, financial budgeting software has become essential for managing financial activities efficiently and accurately. Organizations and individuals rely on these tools to plan budgets, monitor expenditures, and support decision-making processes. However, the growing dependence on such software has also introduced new cyber security challenges. One of the less visible yet highly impactful threats is supply chain attacks, where attackers exploit vulnerabilities in third-party vendors, software components, or updates to gain unauthorized access. These attacks are particularly dangerous because they target trusted sources, making them difficult to detect and prevent. This study aims to examine supply chain attacks as a hidden risk in financial software used for budgeting, with special reference to Coimbatore city. It focuses on identifying potential vulnerabilities, assessing the level of awareness among users, and emphasizing the importance of effective security practices to safeguard sensitive financial information.

1. Objectives:

1. To examine the characteristics and effects of supply chain attacks on budgeting software and understand their influence on the security of financial systems.

2. To determine the major weaknesses and risk elements linked to third-party vendors and external software components used in financial applications, with a focus on Coimbatore city.

3. To assess the awareness and readiness of users and organizations in Coimbatore in dealing with supply chain threats, and to propose suitable measures to strengthen cyber security practices.

II. Statement of Problem

The growing dependence on financial budgeting software has improved the efficiency of financial planning and decision-making. However, it has also introduced hidden cyber security risks, particularly supply chain attacks. These attacks occur when vulnerabilities in third-party vendors, software components, or updates are exploited to gain unauthorized access to sensitive financial data. As these sources are generally trusted, such threats often go unnoticed until significant damage occurs. Many organizations and users lack sufficient awareness and preparedness to address these risks, leading to weak security practices and increased chances of data breaches. In Coimbatore city, the rapid adoption of financial software makes it essential to understand these vulnerabilities and strengthen cyber security measures to ensure better protection of financial systems.

1. Need of This Study

1. To understand the emerging threat of supply chain attacks in financial budgeting software, which is often overlooked by users and organizations.

2. To identify the security gaps and vulnerabilities present in third-party components and external software dependencies.

3. To analyze the level of awareness among users and organizations regarding cyber security risks in Coimbatore city.

4. To highlight the importance of adopting strong security measures to protect sensitive financial data from potential cyber threats.

5. To provide practical suggestions and strategies for improving the safety and reliability of financial software systems.

III. Research Methodology

This study uses a descriptive research design to examine supply chain attacks in financial budgeting software. Both primary and secondary data are collected for analysis. Primary data is gathered through questionnaires and interviews with users in Coimbatore city, while secondary data is obtained from journals, reports, and online sources related to cyber security. A convenient sampling method is used to select respondents. The collected data is analyzed using simple percentage and descriptive methods to understand awareness levels, vulnerabilities, and security practices. The methodology helps in identifying risks and suggesting measures to improve the security of financial software systems.

IV. Review of Literature

Patel (2019): Investigated the level of cyber security awareness among individuals and small businesses. The findings reveal that most users are not fully aware of the risks associated with supply chain attacks and often neglect basic security practices. This lack of awareness leads to weak system protection, making financial software more vulnerable to cyber threats. The study highlights the importance of user education and training.

Johnson and Lee (2020): Focused on the security challenges in financial applications, particularly budgeting software. Their study found that these applications rely heavily on external libraries, plugins, and cloud-based services, which increases their exposure to potential vulnerabilities. The authors stress that insufficient control and monitoring of these third-party integrations can lead to significant security breaches and compromise sensitive financial data.

Smith (2021): Examined the increasing threat of supply chain attacks in modern software environments. The study explains that attackers often target third-party vendors and service providers as entry points into secure

systems. Since organizations place high trust in these external components, malicious code introduced through them can remain undetected for long periods. The research highlights that traditional security measures are often ineffective against such indirect attacks, making them a serious concern for financial software systems.

Kumar (2022): Analyzed cyber security practices among organizations and discovered that many companies do not conduct proper risk assessments of their software vendors. The study points out that the lack of strict vendor evaluation and monitoring increases the likelihood of supply chain attacks. It also emphasizes the need for organizations to adopt structured risk management frameworks to ensure better protection of financial information.

Anderson (2023): Highlighted various strategies to reduce the impact of supply chain attacks on financial systems. The research emphasizes the importance of continuous monitoring, timely software updates, and strict verification of vendors and software components. It also suggests that implementing strong cyber security policies and regular audits can help organizations detect and prevent potential threats at an early stage.

V. Limitation Of Study:

1. The study is limited to a small sample size, which may not represent all users.
2. The research is restricted to Coimbatore city, limiting its wider applicability.
3. The study is conducted within a short time period, affecting detailed analysis.

Supply Chain Attacks in Financial Software:

Supply chain attacks have become a growing cyber security concern in financial software, especially in budgeting applications that rely on multiple external components. These attacks occur when cybercriminals target third-party vendors, service providers, or software dependencies to gain unauthorized access to systems. Unlike direct cyber-attacks, supply chain attacks exploit trusted sources, which makes them more difficult to detect and prevent. Financial software often integrates with payment gateways, cloud platforms, and data processing tools, creating multiple entry points for attackers. If any one of these components is compromised, the entire system may be exposed to risk. Attackers may introduce malicious code into software updates or hidden components, allowing them to access sensitive financial data without immediate detection. This can lead to data breaches, financial losses, and damage to organizational reputation. As digital financial tools continue to expand, the complexity of software ecosystems also increases, making them more vulnerable to such threats. Therefore, it is important for organizations to understand how supply chain attacks work and to take proactive measures to secure their systems. Strengthening security at every level of the software supply chain is essential for protecting financial information and ensuring system reliability.

Security Weaknesses in Budgeting Applications:

Budgeting applications are widely used to simplify financial planning, but they also contain several security weaknesses that can expose sensitive data to cyber threats. These applications depend on various third-party tools, external libraries, and plugins to enhance their functionality. While these components improve efficiency and user experience, they may also introduce vulnerabilities if they are not properly managed or updated. In many cases, outdated software or poorly maintained components can create entry points for attackers. Another issue is the lack of complete visibility into all integrated components within the application. Developers and users may not be fully aware of every dependency, making it difficult to identify and address potential risks. Hackers often exploit these hidden weaknesses to gain unauthorized access,

manipulate financial data, or disrupt system operations. Additionally, weak configuration settings and insufficient security controls further increase the chances of cyber-attacks. To reduce these risks, it is important to conduct regular system audits, update software components, and implement strong security practices. By addressing these weaknesses, organizations can ensure better protection for their financial data and maintain the reliability of budgeting applications.

Awareness and Security Challenges:

A major factor contributing to the risk of supply chain attacks is the lack of awareness among users and organizations regarding advanced cyber security threats. Many individuals focus only on basic protection methods, such as using passwords or antivirus software, without considering risks related to third-party integrations and software dependencies. This limited understanding makes financial systems more vulnerable to hidden attacks. In regions like Coimbatore city, where the use of financial budgeting software is increasing, awareness about cyber security practices is still developing. Small businesses and individual users, in particular, may not have access to proper training or resources to understand these risks. Organizations may also lack clear security policies or fail to implement effective risk management strategies. As a result, potential threats often go unnoticed until they cause significant damage. Improving awareness is essential to address these challenges. Providing regular training, conducting awareness programs, and encouraging safe digital practices can help users identify and prevent cyber risks. When individuals and organizations are well-informed, they are more likely to adopt stronger security measures, thereby reducing the chances of supply chain attacks and protecting sensitive financial information effectively.

Measures to Improve Security:

Enhancing the security of financial budgeting software requires a combination of technical solutions and user-focused strategies. One of the most important steps is to carefully evaluate and select third-party vendors and software components before integrating them into the system. Organizations should ensure that these vendors follow strong security standards and regularly update their software. Regular patching and updating of applications help in fixing known vulnerabilities and preventing exploitation by attackers. Continuous monitoring of system activities is another essential measure. By tracking unusual behavior or unauthorized access attempts, organizations can detect potential threats at an early stage. Implementing strong access control mechanisms, such as multi-factor authentication, can further protect sensitive financial data. In addition, encryption techniques should be used to secure data during storage and transmission.

VI. Case Study 1: Supply Chain Vulnerability in a Coimbatore Financial Software Firm (2025)

Incident Summary:

A medium-sized financial service company in Coimbatore used budgeting software integrated with third-party cloud storage and analytics tools. The system was widely used for managing client accounts, financial planning, and reporting. During a routine update, one of the third-party plugins introduced a hidden vulnerability. This allowed unauthorized access to sensitive financial data, including transaction details and user credentials. The issue remained undetected initially because the software continued to function normally, giving a false sense of security to the organization.

Attack Details:

Attackers exploited the weak security controls of the third-party plugin, which was automatically updated without thorough verification. Once inside the system, they accessed financial records and monitored data flow over a period of time. The attack did not disrupt operations immediately, making it difficult to identify. The breach was discovered only after unusual login attempts and inconsistencies in financial reports were noticed. By that time, a portion of sensitive data had already been exposed.

Critical Lessons:

This case highlights that third-party components can become major security risks if not properly monitored. Organizations should not rely completely on trusted vendors without verification. Regular security audits, controlled updates, and continuous monitoring are essential to prevent such incidents. The study also emphasizes the need for increased awareness and strong cyber security practices among financial software users in Coimbatore.

Suggestions for Improving Security:

Financial organizations should implement strict verification processes before integrating third-party components into their systems. Automatic updates must be monitored and tested in a controlled environment before full deployment. Regular security audits and vulnerability assessments should be conducted to identify hidden risks. Organizations should also adopt strong authentication methods and encrypt sensitive financial data to prevent unauthorized access. Continuous monitoring systems can help detect unusual activities at an early stage. In addition, providing cyber security training to employees and users will improve awareness and reduce the chances of human error. By following these measures, organizations can strengthen their defense against supply chain attacks and ensure safer use of financial budgeting software.

VIII. Case Study 2: Cloud Service Dependency Risk in a Coimbatore Financial Startup (2025)

Incident Summary:

A financial startup in Coimbatore used cloud-based budgeting software to manage customer expenses, billing, and financial reports. The software depended on a third-party cloud service provider for data storage and synchronization. Due to rapid business growth, the company focused more on functionality and less on security checks. During a routine system upgrade by the cloud provider, a configuration weakness was introduced, which created an opportunity for unauthorized access. Sensitive financial data, including user records and transaction details, became exposed without immediate detection.

Attack Details:

Attackers identified the misconfiguration in the cloud service and used it to access stored financial data. Since the cloud platform was directly connected to the budgeting application, the attackers could retrieve information without disrupting the system's normal operations. The breach remained unnoticed for a period of time because there were no strong monitoring mechanisms in place. It was eventually detected when unusual data access patterns and unexpected system logs were observed. By that time, a portion of the data had already been compromised.

Critical Lessons:

This case highlights the risks associated with relying heavily on cloud service providers without proper security validation. Even trusted platforms can introduce vulnerabilities if configurations are not properly managed. Organizations must take shared responsibility for securing their data and systems. Regular monitoring and proper configuration management are essential to prevent such risks.

Suggestions for Improving Security:

Organizations should regularly review and validate cloud configurations to ensure they meet security standards. Access permissions must be strictly controlled to limit unauthorized entry. Continuous monitoring tools should be used to detect unusual activities in real time. Data encryption should be applied both during storage and transmission to enhance protection. It is also important to conduct periodic security audits and risk assessments. Providing proper training to employees on cloud security practices can further reduce risks.

IX. Conclusion

This study highlights the growing concern of supply chain attacks as a hidden risk in financial software used for budgeting. As organizations and individuals increasingly depend on digital tools for financial management, the exposure to cyber security threats has also increased. Supply chain attacks are particularly dangerous because they exploit trusted third-party components, making them difficult to detect and prevent.

The findings of this study show that many users and organizations, especially in Coimbatore city, have limited awareness of these risks and often lack strong security practices. This creates vulnerabilities that can lead to data breaches and financial losses. The study emphasizes the importance of identifying potential risks, improving awareness, and adopting effective security measures.

References

1. Brown, L., & Davis, M. (2020). Cyber security risks in financial information systems. Journal of Financial Technology, 14(2), 88–102.
2. Clarke, R. (2019). Understanding the threats of software supply chain attacks. Computers & Security, 85, 200–210.
3. Evans, P. (2021). Managing third-party risks in digital finance platforms. International Journal of Cyber Studies, 9(1), 33–47.
4. Gupta, R., & Sharma, V. (2022). Cyber threats in financial software and preventive measures. Indian Journal of Cyber security, 6(3), 55–68.
5. Harris, J. (2020). Software vulnerabilities and risk management strategies. Journal of Information Assurance, 11(4), 90–105.