The Evolution of IT Auditing Addressing Increased Vulnerabilities in Online Systems

Matthew Williams

University of The Bahamas

Author Note

This paper was created with the intention to serve as a submission for CISB-410-01 final project.

Abstract

This paper analyzes the transition from batch processing systems to online systems and how it has affected the IT auditing process. It explores how the IT Auditing responses have changed due to the advancements from batch systems to online systems while also highlighting the new risks and vulnerabilities that exist. While elaborating on the ways in which auditing occurred when most devices were batch systems and how it shifted when those devices became online systems connected to the internet. While concluding on which direction auditing should take as it prepares for the future challenges of technological innovation.

Keywords: IT Auditing, Batch Systems, Online Systems, IT auditing standards

Introduction

As companies continue to grow and utilize more advanced computing technologies to store their data, process their information, and complete daily business processes. Companies in the 21st century aim to have social media accounts to increase their presence on a global scale. Some companies utilize their social media accounts as a form of point for customer service to take place, while others utilize it for advertisement purposes. It is now more vital than ever for Information Technology (IT) Auditing to be implemented into the regime of business around the world. IT Auditing can be recognized as a process switch utilized for the evaluation of systems, controls, processes, and information technology systems that affect businesses. It includes but is not like evaluating how efficient, adequate, and effective those systems are in protecting data and complying with industry standards (Tamboly, 2024). However it wasn't always this way as online systems did not always exist as batch systems were the standard, thus this paper aims to analyze how the IT auditing process has shifted due to advancements in technology.

The Advancement of Batch Systems to Online Systems

Batch systems are the systems that preceded online systems which are quite popular today due to their numerous advancements and features which allow for increased productivity in a timely manner. They also allow for remote use which could not be seen before with batch systems. However one time in history individuals truly valued batch systems especially in the corporate world as it allowed the human race at that time to calculate necessary calculations in a time frame, which at the time was recognized as fast. With this in mind, batch systems can be recognized as systems that process large sets of data on a routine schedule. It requires little programming skills to be maintained, computers of the second generation which were produced between 1955 to 1965 were recognized to be built utilizing a single-stream batch processing

system. Companies like IBM Computer and General Motors were notorious for their batch systems which would put all related jobs into batches (also known as groups) and would then send them to the operating system where the punch cards would be punched and finished all at once on a routine basis, based on the prompt given to the system. These systems were centralized systems are the batches would have to be collected to be inputted. This process would be prone to errors due to the medium utilized for input being fragile. In later variations of batch systems, the data would be entered into a file with the use of a terminal and that data would be processed in batch mode (Geeks for Geeks, 2023; Geeks for Geeks Staff, 2022; Cascarino, 2012; Singh, 2023). Due to the style of batch systems, the main control objectives were accuracy and completeness of capture, as once the batch was processed corrections could not be made. Additionally, batch systems would not compute in real-time as the economic event would've had to occur for the data to be placed into the system to be processed (Hall, 2011, p. 252). Thus, in this type of system auditors primarily depended on manual controls and documentation to be able to audit and determine if errors of significance occurred (Pathak, 2005, p. 40). Auditors had to understand and learn the different ways in which the batch systems worked, there were no IT standards, frameworks or guidelines to be followed at the time (Tamboly, 2024). Thus, auditors at the time would utilize test decks to test if the programmers' program worked as it was stated to. Another method used to audit batch systems was the model approach, which is a method where an auditor would formulate a criterion for the system and then its formulation (Boutell, 1965). Systems would continue to evolve leading to multiprogramming systems, then to the current time-sharing systems (Singh, 2023). As the evolution of computers continued eventually online systems were created, systems that would allow the capturing and processing of data to take place online in a real-time environment while still utilizing a minute batch component.

Online systems would gain a new component which placed it in a different category from batch systems, and that would be a communication component that would allow systems to communicate with each other. The auditing process would now have to change as this new component would introduce new vulnerabilities that did not exist prior.

Increased Vulnerabilities in Online Systems

As the world, as a large entity advanced computer systems had to keep up with the advancements to support businesses that were now going global, companies which wanted their stores to have an online presence. Systems of today which are online systems are able to communicate with each other with most using a half-duplex or duplex form of communication. Half-duplex communication allows for two-way traffic to occur, but only one way at a time. Duplex communication allows for communication to occur simultaneously in two-way traffic (Cascarino, 2012). Due to these advancements, individuals can now target the communication component, especially considering that this component would eventually lead to computers connecting to a larger network known as the Internet. The internet would grant those with malicious intentions the capability to attack systems remotely once they had enough skill and manpower as now many devices would operate on the internet to ensure that global communication can occur. Thus, companies would have to utilize safety measures like encryption, which scrambles the data into unread forms until received by the assigned receiver, and protocols, which are a set of rules for the data being transferred (Cascarino, 2012). IT auditing would become more beneficial for companies now more than ever before, as though their data is still in a centralized environment, it is now where users can find it from the comfort of their home countries once they have dedicated enough resources to their goal of finding it.

The Role of IT Auditing in Addressing Vulnerabilities

IT auditing is increasingly more important than ever as companies become more reliant on new technologies for their daily business processes. IT Audits aim to assist with identifying vulnerabilities within the system which can lead to mitigating the risk of data breaches, fraud, and overall downtime for the company's operations (Tamboly, 2024). Auditing is not as linear as it appears and it must make adjustments and advancements as the technology or information it audits does (Teck-Heang & Ali, 2008; Ajao, Olamide, & AyodejiTemitope, 2016). Consequently, as systems gain the capability to connect to the internet, the IT auditing process advances as well. The auditing process would adopt global standards and guidelines which include but are not limited to, COBIT (Control Objectives for Information and Related Technology), ISO 17799, ITIL (IT Infrastructure Library), COSO Internal Control Integrated Frameworks, and COSO Enterprise Risk Management Integrated Framework (Cascarino, 2012). Adopting these guidelines would prevent the auditors from having to assume what the criterion for the process should look like as a global standard would be set. These standards would mitigate the risk of data breaches, and fraud for the company. It also would allow companies to state that they met a standard in the event they were to have a data breach, instead of simply stating that their auditor believed their system was up to standard. Auditors would know to adjust their process of auditing and update it to address the newly discovered threats. Thus the auditor process would now include a planning phase, testing of controls phase, and substantive testing phase. Auditors would start the planning phase by reviewing company documents (their policies, organizational structure, and practices), they would then review the general controls and application controls, concluding this phase with planning to test those controls and procedures they would utilize to do so. The testing of controls phase would begin with the auditor testing the

controls, evaluating the results, and determining how reliant they are. An auditor may utilize a work plan which is usually an Excel document with numerous columns to assist them with this part of the process. Upon completion of the testing of the controls phase, the substantive testing phase would begin. In the substantive testing phase auditors would perform the substantive test, evaluate results, and issue their auditors' report. This report would state what was tested, and what evidence was utilized for findings and conclusions and then present the audit committee, a committee made up of shareholders who appoint the auditor, with recommendations for the system (Hall, 2011). This updated process would allow auditors to test the controls of the new online systems and be able to discover the vulnerabilities that would possibly exist.

Case Studies and Examples

Data breaches have been quite popular throughout recent years with two major ones occurring in recent months prior to the writing of this paper. At the end of March 2024, AT&T would've made an announcement stating that it is currently investigating a data breach that occurred, resulting in 70 million current and former customers' information being leaked into the dark web. Based on information provided by AT&T 7.6 million are current accounts with the remainder (65.4 million) being former customers' accounts. However, AT&T assures the public that the breach has not impacted its operations. The information leaked is said to include social security numbers, names, emails, addresses, contact information, and individuals' dates of birth. The company is currently unable to locate the source of the breach at the time of writing. AT&T is not the only telecommunication company to face such a fate; as in recent years both T-Mobile and Verizon have also been impacted (Seddon, 2024; Veltman, 2024). AT&T's compliance however with auditing standards has allowed them to discover the breach in a timely fashion and inform their customers to change their accounts password for future protection.

Similarly, Roku a popular streaming service, has also been compromised due to a cyberattack with 576,000 of their customers' accounts being affected in 2024 for the second time. The first time the breach occurred in 2024, 15,000 accounts were affected. In both cases, hackers gain access to users' login information and utilize it to make purchases. Roku has since agreed to refund charges to affected users and has reset all affected users' passwords. Users have since been cautioned to utilize passwords that are robust comprising letters, symbols, and numbers in attempts to mitigate future risk (Towfighi, 2024).

Strategies for Effective IT Auditing in Online Systems

With data breaches continuing to occur it is vital to have effective IT auditing practices when using online systems. Auditors should continue to follow global standards and guidelines such as COBIT (Control Objectives for Information and Related Technology), ISO 17799, ITIL (IT Infrastructure Library), COSO Internal Control Integrated Frameworks, and COSO Enterprise Risk Management Integrated Framework to ensure companies are compliant (Cascarino, 2012). Companies should aim to conduct IT audits every 1-2 years depending on how much advanced technology they rely on. Companies should utilize a hybrid auditing style which utilizes both internal and external auditors to prevent a biased audit report when the audit is conducted. They should also utilize auditing tools when testing tools when testing certain business processes to ensure it is tested effectively. Tools include vulnerability scanners which test for weaknesses in the system. Network analysis which analyzes how efficient the network is. Review logs to understand what is occurring throughout the year with the system. Auditors also should have the necessary technical and theoretical skills to understand the result from the tools utilized to ensure the most effective message is communicated with stakeholders to increase the security, compliance, and efficiency of online systems.

Future Directions and Challenges

With the introduction of newer forms of artificial intelligence (AI) and machine learning (ML), the potential to strengthen the IT auditing process now exists. Moving forward, as threats begin to increase due to the amount of data that is uploaded onto the cloud, AI can be utilized to combat this issue. AI-powered tools can be implemented into auditing processes allowing routine monitoring, task, and auditor-like decisions to be made in real time to mitigate future breaches. Machine learning will allow the AI to learn from the logs to understand when unusual behavior is occurring on the system and indicate officials of the company prior to addressing it. AI can also be utilized directly in fighting against cyberattacks by learning from the attacks that have occurred and strengthening areas which has proven to be a vulnerable point that allowed those attacks. Additionally, companies can begin to pivot to more decentralized forms of storage which will increase security. Decentralized storage works by splitting data into numerous data centers which prevent data breaches from being useful to hackers as they would only have a portion of the data they seek (Tamboly, 2024). IT auditing should continue to advance to add these changes to the global standards to ensure future protection of users' data.

Conclusion

As companies continue to grow and utilize more advanced computing technologies, so should the auditing process. History has shown that auditing has adapted to the shift from batch systems to online systems. Thus, users can be hopeful that the auditing process will continue to grow with technological advancements. However, users must hope that it happens soon considering the data breaches which have continued to occur at the time of writing as their data continues to be circulated globally. Users must also remember to utilize advice provided by the

companies that have faced such significant data breaches, by changing their passwords to robust ones.

References

Ajao, O. S., Olamide, J. O., & AyodejiTemitope, A. (2016). Evolution and development of auditing. *Unique Journal of Business Management Research, 3*(1). Retrieved from https://www.researchgate.net/profile/Ayodeji-Ajibade/publication/304115143_Evolution_and_Development_of_Auditing/links/5766da6308aedbc345f5f37e/Evolution-and-Development-of-Auditing.pdf

Boutell, W. S. (1965). Auditing Through The Computer. *The Journal of Accountancy*, 41-47.

Cascarino, R. E. (2012). *Auditor's Guide to IT Auditing.* Hoboken: John Wiley & Sons.

Geeks for Geeks. (2023, December 21). *History of Operating System*. Retrieved from Geeks for Geeks: https://www.geeksforgeeks.org/evolution-of-operating-system/

Geeks for Geeks Staff. (2022, July 8). *Difference between Batch Processing System and Online Processing System*. Retrieved from Geeks for Geeks: https://www.geeksforgeeks.org/difference-between-batch-processing-system-and-online-processing-system/

Hall, J. A. (2011). *Information Technology Auditing and Assurance* (Vol. 3). Mason: Cengage Learning.

Pathak, J. (2005). *Information Technology Auditing An Evolving Agenda.* Berlin: Springer.

Seddon, S. (2024, March 30). *AT&T data breach: Millions of customers caught up in major dark web leak*. Retrieved from BBC: https://www.bbc.com/news/world-us-canada-68701958

Singh, V. (2023, October 13). *Evolution of Operating System*. Retrieved from Shiksha Online: https://www.shiksha.com/online-courses/articles/evolution-of-operating-system/

Tamboly, N. (2024, January 25). *History and Evolution of IT Auditing*. Retrieved from AuditGURU: https://audit.guru/history-and-evolution-of-it-

auditing/#:~:text=The%20roots%20of%20IT%20auditing,discipline%20within%20traditional%20financial%20auditing.

Teck-Heang, L., & Ali, A. M. (2008). The evolution of auditing: An analysis of the historical development. *Journal of Modern Accounting and Auditing*, 1-8. Retrieved from https://www.researchgate.net/profile/Azham-Md-Ali/publication/339251518_The_evolution_of_auditing_An_analysis_of_the_historical_development/links/5e45ec9f458515072d9a7bfb/The-evolution-of-auditing-An-analysis-of-the-historical-development.pdf

Towfighi, J. (2024, April 12). *Roku says 576,000 accounts breached in cyberattack*. Retrieved from CNN Business: https://edition.cnn.com/2024/04/12/business/roku-security-breach-user-accounts/index.html

Veltman, C. (2024, March 30). *Millions of customers' data found on dark web in latest AT&T data breach*. Retrieved from NPR: https://www.npr.org/2024/03/30/1241863710/att-data-breach-dark-web