THE HACK ATTACK AT WINTER'S TALE PUBLISHING: THE FORENSIC ACCOUNTING/INTERNAL AUDITING PERSPECTIVE

Leisa Marshall, Southeast Missouri State University
Dana Schwieger, Southeast Missouri State University
Christine Ladwig, Southeast Missouri State University
Sandipan Sen, Southeast Missouri State University

CASE DESCRIPTION

The primary subject matter of this case concerns the vulnerabilities that poor management can expose an organization to as well as the widespread effects that a hacker attack can have on a business' operations. Secondary issues examined include, auditing frameworks to evaluate internal controls, designing a secure network for small start-up businesses, and addressing legal and marketing concerns of a hacked organization. The case has a difficulty level of three or higher and was designed to be taught in a 30 to 45 minute time period with approximately two hours of outside preparation by students. The case can be approached from five perspectives (management, business law, information technology management, forensic accounting and marketing), thus the case can be used in multiple 30 to 45 minute classes. Instructor's notes from each of these perspectives have been written to allow for an integrated approach to learning across the curriculum. The following set of teaching notes evaluates the case from a forensic accounting/ internal auditing perspective.

Evaluation of the case from a forensic accounting/internal auditing perspective requires the application of AU §316, Consideration of Fraud in a Financial Statement Audit, the AICPA/Canada Trust Services and Principles, and COSOs Integrated Framework to the facts of the case. The case from a forensic accounting/internal auditing perspective is primarily designed for junior or senior-level undergraduate students majoring in accounting with a basic knowledge-base in internal controls.

CASE SYNOPSIS

The case describes Winter's Tale Publishing, an online startup publishing house started by John Winters after successfully publishing his own book. The organization grew quickly but cut corners in several areas which would later come to haunt them. Winter's Tale started a marketing campaign to build interest in a soon-to-be-published tell-all book. Controversy surrounded the publishing of the book and hackers attacked Winter's Tale's server. The hackers accessed personal client author information as well as employee emails and posted the information online for all to see. The case ends with John and his staff meeting to evaluate the circumstances, control the damage, implement a strategy going forward, and determine what led them into such a susceptible state.

STUDENT LEARNING OBECTIVES

The case can be examined across a business program in multiple courses to provide students with a holistic approach to evaluating the ramifications of business decisions to multiple dimensions of an organization. The case can also be addressed in an individual course. Upon reading, analyzing and discussing the case from the accounting/internal control perspective, students should be able to:

1. Demonstrate an understanding of internal control concepts related to fraud risk factors of AU §316 and objectives, components, and principles of the COSO's Internal Control-Integrated Framework (2013).
2. Apply analytical and critical thinking skills as they analyze the case to identify internal control deficiencies and recommend mitigating internal controls to address the deficiencies.
3. Evaluate the case from the perspective of the Integrated Framework's objectives, components and principles and from the perspective of the AICPA/CPA Canada Trust Services Principles and Criteria.

RECOMMENDATIONS FOR TEACHING APPROACHES

The case can be taught from multiple perspectives in several different courses such as upper level marketing, business strategy, business law, human resources, forensic accounting/auditing, and information technology management. The following case notes address the issues from the perspective of forensic accounting/ auditing. Case coverage should take approximately 30 to 45 minutes of course time. Senior level students may be asked to analyze and write up the case using a case analysis template such as:

Background
Main Problem
Minor Problems (stemming from main problem)
Possible Solutions
Recommended Solution and Implementation
Recommended Precautionary Measures and Implementation (What should have been done to prevent this situation?)

Possible forensic accounting/internal auditing questions that may be provided to students include the following:

Target courses: Forensic Accounting, Internal Auditing, Financial Auditing

1. *Define fraud. Describe the difference between fraud and errors as defined in AU §316,* ***Consideration of Fraud in a Financial Statement Audit.*** *What are the two types of misstatements relevant to the independent auditor's consideration of fraud? As the independent auditor of Winter's Tale Publishing, identify whether you believe the hacking was a fraudulent act, an error, or neither.*

In general, fraud is the intentional deception in which the perpetrator receives financial or personal gain. According to AU §316.05, the difference between fraud and an error depends on intent to materially misstate the financial statements. Fraud is an intentional act to materially misstate the financial statements.

The two types of misstatements relevant to the external auditor include (1) misstatements arising from fraudulent financial reporting and (2) misstatements arising from misappropriation of assets. Both types of misstatements cause the financial statements to be in nonconformance with generally accepted accounting principles (GAAP).

2. *Describe the fraud risk factors identified in AU §316 as the risk factors relate to John Winters and Will Martin.*

The three risk factors include incentive or pressure, opportunity, and rationalization or attitude. Pressures describe the reasons that fraud is committed. Opportunity is the existence of circumstances which allow fraud to be committed. Most often, these circumstances result from a lack of internal controls. Rationalization is the perpetrator's ability to justify and intentionally commit a dishonest act.

John's apparent successes had recently been met with a six-month drought of clients cancelling. In addition, John had invested most of his income in the business; he was attempting to make a name for himself, and had bills backing up with payroll to meet. The opportunity for John to commit this fraud existed only with the assistance of Will, the IT expert. Evidence of this opportunity does not exist.

Will's access to all of Winter's Tale's IT, provides Will the opportunity to create the current situation. John had conveyed all IT activity to Will, including all of the Internet access, networking, and website hosting. Given Will's prior conviction of computer tampering, Will may not have needed pressure or rationalization. He may have simply enjoyed the thrill of computer tampering. Will may also have been frustrated at John's inattentiveness to the unusual activity regarding the IP addresses. However, Will's multiple attempts to address the unusual activity with the particular series of IP addresses and Will's desire to hire a security expert to evaluate the IT system, might imply that he was attempting to divert the situation at hand.

3. *The AICPA/CPA Canada's Trust Services Principles and Criteria address security, availability, processing integrity, confidentiality, and privacy for assurance on information technology-enabled systems. Define the five criteria and identify which of the five listed criteria were violated?* http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/trustdataintegritytaskforce.aspx

The principle of security refers to the protection against unauthorized access. The hacking that occurred clearly indicates that the system was not secure. The security criteria were violated. Availability refers to access to the system and processing integrity refers to the valid, complete, accurate, timely and authorized transactions. These two criteria do not appear to have been violated. Confidentiality refers to the company's information; whereas privacy refers to personal information. Both of these were certainly violated with the publishing of information to the social media URL.

4. *According to the Committee of Sponsoring Organizations Internal Control Integrated Framework (COSO-updated May 2013) three categories of objectives exist for an organization's internal control efforts. These objectives include (1) Operations, (2) Reporting, and (3) Compliance. Discuss these objectives from the perspective of Winter's Tale Publishing meeting these objectives. COSO's Framework* http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf

The COSO *Integrated Framework* defines Operations Objectives as those that "pertain to effectiveness and efficiency of the entity's operations, including operational and financial performance goals, and safeguarding assets against loss." The hacking into the company's information system clearly indicates that assets were not properly safeguarded. Information specific to the company and the company's customers was the main "asset" that was not safeguarded. The lack of safeguarding their customers' information indicates Winter's Tale Publishing has not met their Operations Objectives.

The Reporting Objectives relate to both internal and external financial and non-financial reporting. Compliance Objectives refer to adhering to laws and regulations. Although a lack of apparent violation of the Reporting Objectives exists, the Compliance Objectives are likely to have been violated, as personal customer information (full names, social security number, and bank account numbers) was provided to the public on company's social media URL.

5. *The COSO's Integrated Framework suggests the need of five critical components and 17 principles to assess the effectiveness of internal controls. These controls include the control environment, risk assessment, control activities, information and communications, and monitoring. Which of these components, if any, appears to be lacking at Winter's Tale Publishing? Which COSO objective links to the hack of Winter's Tale Publishing's computer system?*

The risk assessment and control activities components appear to be lacking. Risk assessment requires the evaluation of potential threats that would adversely affect the company. The risk of hackers to the system and contingency plans should be in place. The hack created a direct threat and damages to the effective and efficient operations at Winter's Tale Publishing, providing a direct link to the lack of operations objectives.

6. *In an effort to evaluate the current situation with the hack, the auditor brought in by Winter's Tale Publishing decided to evaluate their internal control system based on the COSOs Integrated Framework. Assume as a first step in the process, Winter's Tale Publishing establishes the operations objective to "s**afeguard client information from unauthorized access, use, and dissemination**." As the auditor, continue the evaluation of the situation, using the Framework's components and principles, to identify internal control deficiencies and measures that should be taken to prevent and/or detect hacks in the future.*

The components are listed in question #5. Students should methodically identify the principles within each component that lead to the identification of internal control deficiencies. See Table 1 for a summary of internal control deficiencies and mitigating internal controls.

The **control environment** refers to the "tone at the top" and the "standards, processes, and structures that provide" the foundation for the internal control structure across the organization. Five principles are associated with the control environment with two principles that directly relate to the situation at Winter's Tale Publishing. Winter's Tale Publishing did not **provide for "appropriate authorities and responsibilities** in pursuit of the" objective to safeguard client information. The situation is such that John relegated complete authority of the information system to Will. Will was at liberty to develop a system, on the low-budget side, possibly forgoing critical applications and safeguards relevant to access to the system. The second principle that was not adhered to was **"a commitment to attract, develop, and retain competent individuals."** The lack of a background check on Will provides little evidence that John was objective in his decision to hire

ill, instead relying on what he "felt" during the interview process. At a minimum, John should adopt better hiring practices by obtaining background checks, including criminal, on potential employees. Given the sensitive nature of client information and the need for a true information system's expert, John also should have investigated Will's credentials.

The **risk assessment** component requires the identification of risks that could prevent the achievement of the objectives. The four principles associated with the risk assessment component provide for the iterative process in the identification and assessment of threats to meeting the objective stated above. In general, the risk assessment principles include (1) the identification of the risks of the objectives not being met, (2) an analysis of the risks (and potential responses), (3) the consideration of fraud, and (4) assessing the impact of significant changes that would affect the internal control system.

The most relevant principle related to the risk assessment component includes an analysis of the risks (and related responses). An analysis of the potential vulnerabilities of the information system would have led to the identification that the system could be hacked and client information obtained. Assuming this risk was at a level high enough to warrant action, control activities would have been implemented to prevent the threat. In addition, an appropriate response to the occurrence of the hack, would have been documented in a disaster recovery plan. Given the small size of the company, three individuals, John should have decided that the risk of a hack was too large, and decided to outsource his information technology needs instead of keeping it in-house.

The **control activities** component refers to specific policies and procedures that serve to mitigate risks of the objective(s) not being met. Control activities apply to the organization as a whole, to business processes, and to the technology environment. The three principles include (1) the selection and development of control activities to mitigate risks of achieving objectives, (2) the selection and development of control activities over technology, and (3) the implementation of control activities.

The initial response by students to specific control activities to mitigate the risk at Winter's Tale Publishing will probably be the implementation of segregation of duties. However, with only three people in the organization, each with an expertise in their respective areas but not in the other areas, segregation of duties is not feasible. However, at a minimum, John should obtain a minimum working-knowledge in all areas within his business. In addition, an evaluation of the system would have highlighted the need for alternative controls to achieve similar results as segregation of duties. The identification of the segregation of duties may have led to possibly outsourcing the IT function or hiring a CPA to evaluate the system based on the Trust Services Principles and Criteria ®.

The obvious principle that appears to have been overlooked is the implementation of control activities over technology. Several general controls exist that John should oversee. Specific general controls include authentication controls whereby only authorized users with unique user IDs and passwords have access to the system. Approved users should appear on a list, with each access compared to the computerized list prior to access being allowed. Unauthorized access should be flagged immediately, with a shut-down of the system to prevent further damage. Finally, a third-party verification, such as that provided by CPAs and based on the AICPA/Canada Trust Services Principles and Criteria, of the proper working of the controls within the system should be implemented.

The **information and communication** component refers to obtaining relevant information (both internal and external) to support the functioning of internal controls. Due to the lack of internal control, an internal control deficiency exists with this component. After establishing and implementing an internal control structure, John should ensure that relevant information is obtained and communicated both internally and externally. Regarding the breach of Winter's Tale Publisher's clients' personal information, the method of communicating with clients (external parties) should follow all legal requirements.

The **monitoring** component principles include (1) the "ongoing and/or separate evaluations" of the internal controls and whether they are properly functioning and (2) the timely communication of internal control deficiencies. Evidence of monitoring activities exists with Will's identification of "increasing amount of unusual activity occurring from a particular series of IP addresses." However, this basic monitoring activity went unnoticed by John, who was "too busy finishing the book and kept missing meetings with Will." John obviously should have met with Will to address the potential breach in the system.

Table 1
SUMMARY POINTS OF DEFICIENCIES AND MITIGATING MEASURES TO PREVENT AND/OR PROVIDE EARLIER DETECTION

INTERNAL CONTROL DEFICIENCY	MITIGATING MEASURE/INTERNAL CONTROLS
Control environment	
Poor hiring practices	Background checks to include criminal, work history, educational credentials
Improper assignment of authority and responsibilities	John should take responsibility with respect to the operations of the IT function within Winter's Tale Publishing. John might consider outsourcing the IT function.
Risk Assessment	
Lacks a risk assessment process	Implement a risk assessment process, taking into consideration the principles identified in the COSOs Integrated Framework
Control Activities	
Lacks segregation of duties	Outsource the IT function Hire an independent CPA to provide a Trust Services engagement, with a specific focus on evaluating the IT system's security and privacy Access controls
Possible unauthorized access	Access controls to include user IDs and passwords Access control log with unauthorized access attempts logged – follow-up on log reports
Lacks authorization controls	Create a computer-generated matching of approved users and availability of the systems data, files, etc.
Information and Communication	
Lacks a system for identifying relevant information to receive and disseminate information regarding the proper functioning of internal controls	Develop policies and procedures for obtaining and disseminating information
Monitoring	
Lack complete monitoring of internal controls	John should drop all activities and meet with the IT person immediately. The strange activity that occurred and was noted by Will, should have been investigated much earlier.