Early-stage paper

The White-Collar Hacking Contest:
A Novel Approach to Teach Forensic Investigations in a Digital World

Michael Schermann
Technische Universität München
Information Systems (I17)
Boltzmannstrasse 3
85748 Garching, Germany
+49 89 289 19507
michael.schermann@in.tum.de

Scott R. Boss
Bentley University
Department of Accountancy
175 Forest Street
Waltham, MA 02452, USA
+1 781 891 2353
sboss@bentley.edu
The White-Collar Hacking Contest:
A Novel Approach to Teach Forensic Investigations in a Digital World

Abstract

This paper presents the rationale, elements, and process of the white-collar hacking contest (WCHC), a novel approach to teach forensic investigations, management controls, and security in the digital environment. The WCHC is a round-based contest, where participants in turn act as those who commit fraud (fraudsters) and forensic investigatory teams. State-of-the-art enterprise information systems serve as the playing field for the game. The contest was developed in close cooperation with experienced forensic investigators to ensure real-life conditions for both fraudsters and forensic investigators. This serious gaming approach helps to advance teaching on fraud detection and forensic investigations in the digital age in two important ways. First, it provides an intriguing way to teach forensic investigation methods to students of interdisciplinary backgrounds. In particular, students experience the role of both a fraudster and a forensic investigator. Second, the contest design helps to focus on ambivalent fraud schemes where a number of possible legal alternatives can be presented to rebut the gathered evidence. We also discuss the WCHC as a starting point for experimental research in fraud investigation.
The White-Collar Hacking Contest: 
A Novel Approach to Teach Forensic Investigations in a Digital World

INTRODUCTION

White-collar crime, or fraud, makes the headlines in newspapers around the globe with a disturbing regularity (Abbasi et al. 2012; Albrecht et al. 2008). While typically only the biggest cases make headlines, the Association of Certified Fraud Examiners (ACFE) shows that fraud is an everyday phenomenon, is committed at all levels in the organization, and is not only confined to groups of greedy senior executives (Association of Certified Fraud Examiners 2012). In a survey from 2012, the ACFE found that the median loss per fraud case was $140,000, while the overall distribution of losses remained on levels similar to those reported in previous surveys (Association of Certified Fraud Examiners 2012). Furthermore, the ACFE shows that fraud schemes become particularly costly to an organization if multiple fraudsters collaborate (Association of Certified Fraud Examiners 2012).

Enterprise information systems play an important role not only in detecting but also in committing fraud (Pearson and Singleton 2008). Modern enterprise information systems provide integrated databases that contain every transaction ever made in the organization, access controls that reflect the organizational structure, and workflows that reflect the organizational processes. Forensic investigators analyze enterprise information systems to identify unusual transactions and weaknesses in the access controls or workflows—transactions which may serve as an indicator for fraud schemes. Additionally, systems auditors and information security specialists work with both the accounting and information systems (IS) functions to test these controls and to close possible access points for individuals to commit fraud. Regardless of the effort expended in such analysis, research has shown that
it typically takes between 12 to 36 months to detect committed fraud schemes (Association of Certified Fraud Examiners 2012).

Why is this the case? It would seem that a centralized control of transactions and systems would create a more secure environment, but employees continue to commit fraud. One possibility is that modern enterprise information systems and technology are now providing a new playing field for fraudsters. Fraudsters can camouflage their fraudulent activities among the millions of existing legitimate transactions without leaving a paper trail. Additionally, fraudsters exploit weaknesses in both the access control mechanisms of systems and the workflows of these enterprise information systems. Without suspicious facts or tips, forensic investigators are tasked with finding the needle in the haystack. Furthermore, suspicious transactions are not enough to make a credible case for fraud within an organization. Forensic investigators face the challenge of collecting enough strong evidence to differentiate between fraud and false positives. They additionally need to work with the IS and information security groups to understand the details of any given exploit (Idziorek et al. 2012). Not surprisingly, the ACFE survey shows that most fraud cases will be detected only through tips from other members of an organization (Association of Certified Fraud Examiners 2012).

Effective forensic investigations need an interdisciplinary approach (Kranacher et al. 2008) if we are to effectively deter and detect fraud at the organizational level. Obviously, forensic investigators need a strong background in accounting, security, and management (Meier et al. 2010). Furthermore, forensic investigators need the capabilities to investigate enterprise information systems controls and security and to apply data analysis techniques to identify suspicious transactions and weaknesses in existing controls (Digabriele 2008). Most importantly, forensic investigators need to understand the behavior of fraudsters (e.g., activities intended to camouflage fraudulent activities) and need to be able to combine this
understanding with the aforementioned skills to discover evidence to establish conclusions that fraud has occurred regardless of the assertions of those under investigation.

The white-collar hacking contest (WCHC) is a novel teaching approach which allows students to experience the perspective and the behavior of both fraudsters and fraud investigators in an environment with an enterprise resource planning (ERP) system. It additionally helps students discover evidence of fraud while acting as an interdisciplinary team of forensic investigators in a close-to-real-world environment. In each round of the WCHC, students are required to get in character as both fraudsters and forensic investigators and compete against each other. The role of fraudster requires students to attempt to camouflage their illegal activities, while the role of forensic investigator requires that students utilize their accounting, security, and systems knowledge to try to uncover any fraudulent activity by the opposing team. The key to success in the WCHC is combining skills in accounting and management with the forensic capabilities to investigate enterprise information systems and establish credible evidence of fraud, even when facing highly ambiguous cases.

In this paper, we explain the design rationales of the WCHC as a holistic approach to teach forensic investigators and enable students to walk in the shoes of a fraudster. We also report on the results from the latest installment of the WCHC at a German university. We discuss the implications of running the WCHC and suggest worthwhile avenues to advance and improve the WCHC for both forensic investigation and organizational information security awareness training.

THE WHITE-COLLAR HACKING CONTEST

The WCHC is designed as a semester-long course for students at either the undergraduate or graduate level. The overall objective of the course is to create a learning environment that resembles a real-world situation where students can experience the work of forensic investigators.
forensic investigation teams. Also, students experience what it is like to be a fraudster by developing a fraud scheme and interacting with forensic investigators.

**Learning Objectives**

Students should have been trained in the basic principles of management, accounting, and security. Previous experience with enterprise information systems is preferable but can also be taught in tutorials. The WCHC helps teachers of forensic investigation to pursue three learning objectives:

1. Understand the principles of fraud detection
2. Gain experience in working with teams
3. Gain an understanding of fraud execution (to be able to accomplish #1 above)

Upon completing the WCHC, students will understand and have applied the principles of fraud detection and forensic investigation in a real-world integrated enterprise information system. Students will understand the structure and configuration of important database tables, access control mechanisms, and workflows of enterprise information systems. Furthermore, students will be able to utilize and evaluate data analysis techniques and be able to choose the most appropriate techniques to detect specific frauds. Most importantly, students will be able to establish a relationship between business activities and their representation in enterprise information systems and will be able to critically investigate this relationship.

Second, students will obtain experience in working on a forensic investigation team and will understand the basic principles of organizing and managing a forensic investigation project. Forensic investigation is an interdisciplinary work involving financial investigators, auditors, and IS personnel. Thus, students will learn how to collaborate with students from different backgrounds and combine their capabilities to achieve the objectives of the contest. Students will learn how to set up and maintain a team structure with clear responsibilities, and over the course of the term will inevitably experience the conflicts, time pressure, and other
various obstacles that need to be resolved within any team endeavor. Furthermore, students will gain experience in how to use results from data analysis to explain an identified fraud scheme and how to develop a compelling case for both reports and presentations for management or law enforcement. Finally, the students will learn how to present their findings and how to interact with alleged suspects.

Finally, the WCHC will enable students to understand the basic principles of developing a fraud scheme and implementing this fraud scheme in an enterprise information system. They will understand how to people with fraudulent intentions will exploit regular business activities. Furthermore, they will gain experience in how to camouflage their fraudulent behavior, as well as their activities in developing and testing their fraud scheme. In particular, students will understand how to develop ambivalent fraud schemes, where data analysis alone does not provide strong evidence. The objective is to have the students develop cover-up stories, which establish alternative, non-fraudulent explanations for the results of the forensic investigators’ data analysis. While it cannot and should not be the objective of the WCHC to train future fraudsters, it is of utmost importance for students to gain an understanding of how a fraudster both thinks and behaves in the course of committing fraud. We believe that walking in the shoes of a fraudster is a key element in training effective forensic investigators.

**Design Rationales**

In pursuit of the learning objectives, we designed the WCHC as an interdisciplinary serious game in which students work in teams that alternate between the role of a fraudster and the role of a forensic investigator (Liu et al. 2013). Six important design rationales are important to pursue the learning objectives in a structured and repeatable way.

First, interdisciplinary team composition is crucial for forensic investigation in the digital environment. Successful forensic investigation teams have a broad range of skills and...
capabilities in the areas of accounting, management, project management, information systems, computer science, and information security. Thus, we announce the white-collar hacking contest in the business school and the computer science school to students of business, computer science, and information systems. Furthermore, we assign the students to teams in a way that ensures that each team has an interdisciplinary mix of skills and capabilities.

Second, forensic investigation teams usually work with client organizations in a highly self-reliant manner. Once we have assigned students to their teams, the students are required to establish a team structure and to organize their project in the way they see as most efficient given their resources. They have to elect a team leader who handles the communication with the instructors of the WCHC and the other teams. The instructors of the WCHC serve as the sponsor of the forensic activities. Thus, the team lead has to inform the instructors about the progress of the forensic analysis (and the implementation of the fraud scheme). This ensures that the instructors keep in touch with the teams and can assist with technical problems and issues not directly related to the assignments.

Third, the WCHC is a round-based contest, which allows us to structure the class and highlight a particular aspect of forensic investigation work in each round. Additionally, the round-based approach helps to adjust the level of difficulty and complexity of the WCHC to the skills and capabilities of the participating students. In each round, teams first develop a fraud scheme and implement it in an enterprise information system. Then, the instructors create database dumps of the teams’ enterprise information systems and swap the data sets among the participating teams. Anonymous swapping is useful in early rounds of the contest. In later rounds, open swapping of data sets makes the task more challenging as inferences can be drawn based on experience and data analytics performed in the previous rounds.

Fourth, each round ends with formal team presentations. Each team first presents the results of their forensic investigation work on the data set they received. Once they have
established their argument, the team that created the fraud scheme in the particular data set presents the details of their fraud scheme and provides an alternative explanation for the forensic results. When each team has presented their argument, the whole class discusses which team has made the more compelling case and whether the forensic results would have been sufficient to convict or warrant additional investigation of the fraudsters. It is particularly vital that experienced forensic investigators participate in the presentation sessions to provide the real-world perspective.

Fifth, student teams compete against each other in the WCHC. As noted earlier, it is not the objective of the WCHC to train future fraudsters, therefore only their work as forensic investigators determines the winners of the contest. Hence, in order to win the contest, the team must identify the fraud case, explain the fraud scheme, and present strong evidence. However, since each team alternates between the role of fraudster and investigator, winning the contest is also a function of creating a believable fraud scheme that opposing teams will either not be able to uncover or which will not provide sufficient evidence to be considered fraud by the judges. This incentive structure helps to put the focus on the forensic work (otherwise their team will not advance in the contest) but also creates sufficiently challenging fraud schemes (otherwise the other teams will also advance in the contest). This incentive structure helps to avoid collusive behavior between teams.

Sixth, grading is not based on whether the students actually were able to commit fraud or were able to identify fraud in the data set of another team but rather on how well they are able to explain, assess, and document their forensic investigatory work and their fraud schemes. This focus on systematic, comprehensive, and reproducible work is important as it reflects the underlying qualities of highly professional forensic investigations.

**Setup**
The setup for the WCHC consists of creating an environment that resembles a real-life organization suitable for being investigated by a forensics team, and also provides the flexibility that is needed to guide and manage student activities. Each team is equipped with two instances of an SAP ERP 6.04 system. SAP ERP systems are enterprise information systems that are in widespread use in organizations around the globe. SAP has the largest market share of all of the ERP solutions worldwide (Columbus 2013).

Students use their first instance of SAP ERP to develop and actually commit their fraud scheme. When swapping data sets between teams, the instructors create a database dump of each team’s first instance and load it to the second instance as the company that the next team is supposed to investigate. After each round of the WCHC, this first SAP ERP instance is reset to make sure that multiple fraud schemes do not overlap. This additionally gives students the opportunity to rethink and revise their techniques for camouflaging their fraudulent actions. As noted, the second instance of SAP ERP for each team is for investigating, analysis, and testing during the forensic phases.

Each SAP ERP instance is prefilled with a data set from a model company called IDES. IDES is provided by SAP for training and educational purposes with a particular focus on the procure-to-pay activities and processes in the SAP ERP systems. The IDES data set provides a reasonable volume of both master data (e.g., suppliers and employee data) and transactional data (e.g., materials and purchase orders). This allows students to camouflage their actions and also enables forensic analysis without extremely complex data analysis techniques. The database tables of the IDES model company can be analyzed with standard Microsoft Office tools.

The SAP ERP instances also come with a set of rules of engagement that help to maintain a certain degree of control over students’ activities. Fraudulent activities are restricted to a specific company code (‘1000’) and to the current financial year. This means that simply sorting the tables by date leads the teams to the fraudulent activities. While
appearing counterintuitive, this helps to focus the student work in the WCHC on explaining fraud schemes from a business perspective and on collecting strong evidence that helps to implicate the fraudulent team rather than searching the database for select transactions. As fraudsters, students know that finding their activities in the dataset is relatively easy for the investigating team, but explaining how those activities are fraud to management or law enforcement should be difficult. The students are allowed to create bogus transactions to camouflage their fraudulent activities but, again, they also should be able to explain their camouflaging activities with legitimate business activities.

Data analysis is a key aspect in forensic investigations. However, extracting data from a production SAP ERP instance is a delicate and time-consuming effort. In the forensic investigation phases, students are given a standard set of data base tables. We allow teams to request additional database tables which they deem necessary for their investigation. To mimic production environments, requesting additional tables means additional waiting time and additional analysis work. Given the tight timeframes for analysis within each round, this ensures that students refrain from simply requesting the whole data set.

**Process**

The WCHC is structured into three main phases. In the first phase, the instructors introduce the students to the foundations of forensic investigation and working with SAP ERP systems. Furthermore, the students learn the definition of fraud and discuss recent publicized fraud cases.

The second phase consists of three or more contest rounds. Each round begins with a fraud phase (where each team develops a fraud scheme or schemes and implements it in their SAP ERP instance) followed by a forensic investigation phase (each team gets the dataset of another team for investigation). Each round is completed with a presentation session, where teams present their evidence and discuss the results.
As the contest progresses, the rounds in the second phase should become more challenging to the teams. For instance, in the first round, we typically have the fraud schemes be presented by the instructors, as students will be challenged enough to implement them and come up with the appropriate analysis techniques to investigate those types of fraud. In the second round, the students should be required to develop their own fraud schemes that work within the pre-defined set of access controls. Finally, in the third round, fraudsters are required to siphon a specific amount of money out of the organization and are allowed to use as many fraud schemes as they like to obtain this objective. Similarly, the forensic investigators are required to identify and explain as many fraud schemes as possible. The specific objectives of each round can be flexibly chosen by the instructors to guide and challenge the students.

The third and final phase of the WCHC is the finale. Students present their overall achievements and discuss the implications of their learning with the instructors and experienced forensic investigators from industry partners. At this point the overall points are determined and the winning team is awarded. The finale can be set up as a session that is open to the public.

Table 1 shows a template for conducting the WCHC.

Table 1: Template for conducting the white-collar hacking contest

<table>
<thead>
<tr>
<th>Phase</th>
<th>Week</th>
<th>Description</th>
<th>Assignment &amp; Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
<td>Kick off (1.5h)</td>
<td>Assignment 1:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Define fraud and forensic investigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Analyze a publicized fraud case</td>
</tr>
<tr>
<td>Contest</td>
<td>4</td>
<td>Course work:</td>
<td>Assignment 1 is due</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Introduction to fraud forensics</td>
<td>Assignment 2:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(3h)</td>
<td>• Be a fraudster: implement a given fraud case</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Introduction to SAP ERP 6.04</td>
<td>Assignment 2 is due</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(3h)</td>
<td>• Submit documentation of fraud case (report, presentation, data set)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Tutorial IDES (2h)</td>
<td>Assignment 3:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Be a forensic investigator; investigate a given data set</td>
</tr>
</tbody>
</table>
## RESULTS OF THE WHITE-COLLAR HACKING CONTEST

In the following, we present the results of the latest installment of the WCHC at a German university. The contest was offered in the school of business and the school of computer science of this university as an elective course.

### Participants

Eleven students participated in the WCHC, with eight students from the business school and three students from the school of computer science. Students were either in the last semester of their bachelor studies or in the second semester of their master studies. Students were assigned to three teams and each of the three students from the school of computer science was allocated to a different team. Students did not have extensive prior experience.

<table>
<thead>
<tr>
<th></th>
<th>First round presentations</th>
<th>Assignment 3 is due:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Submit documentation of forensics project (analysis, report, presentation, data set)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assignment 4:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Develop and implement a fraud scheme</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Second round presentations</th>
<th>Assignment 5 is due:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Submit documentation of forensics project (analysis, report, presentation, data set)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assignment 6:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Develop and implement fraud schemes that siphon off a given amount of money</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Third round presentations Industry talks Winner announcement</th>
<th>Assignment 7 is due:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Submit documentation of forensics project (analysis, report, presentation, data set)</td>
</tr>
</tbody>
</table>
with SAP ERP enterprise information systems or forensic investigation. All students had, however, prior experience with basic data analysis techniques.

**Assignments and Deliverables**

Table 2 presents an overview of the implemented fraud schemes and the results of the forensic analyses. In the first round, we assigned the fraud scheme (fictitious expenses) to the students. Interestingly, the students varied widely in their implementation of this specific fraud scheme. Team 1 reused an already existing supplier while team 3 claimed fictitious expenses with services, which are hard to investigate once consumed. The fraud schemes in rounds 2 and 3 became more elaborate and thus harder to detect.

**Table 2: Overview of fraud schemes committed by student teams**

<table>
<thead>
<tr>
<th>Team</th>
<th>Round 1</th>
<th>Round 2</th>
<th>Round 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Team 1</td>
<td>• Fictitious expenses (with company that exists in the master data)</td>
<td>• False refunds • False exchange rates for orders abroad</td>
<td>False purchasing and receiving (€30,000.00) Overstated expenses (€69,972.00)</td>
</tr>
<tr>
<td>Team 2</td>
<td>• Fictitious expenses (with company that does not exist in the master data)</td>
<td>• Sales scheme with factory abroad</td>
<td>False sales and shipping (€56,767.30) Fictitious expenses with services (€43,232.70)</td>
</tr>
<tr>
<td>Team 3</td>
<td>• Fictitious expenses with services (with company that exists in the master data)</td>
<td>• False declaration of shipping costs for just-in-time delivery</td>
<td>Write-off scheme (€58,090.62) False declaration of goods and false declaration of sales tax (€30,845.00)</td>
</tr>
</tbody>
</table>

Finally, in round three, the teams were asked to siphon off €100,000 from the IDES organization and were allowed to use as many fraud schemes as necessary to accomplish the task. Column 3 of Table 2 shows the actual amount of money that was siphoned off.

Table 3 shows the results of the investigative efforts by each team, indicating both the identity of the team being investigated and whether the investigating team was able to provide conclusive evidence. In round 1 and round 2 all fraud cases were identified and the students applied the appropriate data analyses (i.e., investigated the correct tables). However, in two
cases the teams came forward with evidence that could be explained by the team that had committed the fraud. In the case where Team 2 investigated the data set of Team 3 in round 1, Team 3 basically explained the transactions with the intangibility of services and simply claimed that the services had been delivered.

Table 3: Results of the forensic investigation projects

<table>
<thead>
<tr>
<th></th>
<th>Round 1</th>
<th>Round 2</th>
<th>Round 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Team 1</td>
<td>Team 2</td>
<td>• analyzed</td>
<td>• analyzed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• identified</td>
<td>• suspicious</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• convicted</td>
<td>activities</td>
</tr>
<tr>
<td>Team 2</td>
<td>Team 3</td>
<td>• analyzed</td>
<td>• analyzed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• suspicious</td>
<td>• identified</td>
</tr>
<tr>
<td></td>
<td></td>
<td>activities</td>
<td>• convicted</td>
</tr>
<tr>
<td>Team 3</td>
<td>Team 1</td>
<td>• analyzed</td>
<td>• analyzed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• identified</td>
<td>• identified</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• convicted</td>
<td>• convicted</td>
</tr>
</tbody>
</table>

In round 2, Team 3 developed a fraud scheme that was particularly difficult to investigate. Team 3 created purchase orders for ordering special pumps in England and set up the terms of delivery to state that shipping was included in the orders. However, Team 3 still contracted a shipping company to ship the pumps to Germany. This shipping company was in the control of a friend of Team 3 and no shipping was conducted. Team 3 paid the additional shipping costs, and the additional shipping costs of €4,916.10 were siphoned off the IDES company.

During the investigation phase, Team 1 correctly analyzed and interpreted the activities of Team 3 but disregarded them as camouflaging behavior. They did, however recommended an additional interview with Team 3. Team 3 explained the additional shipping cost with the argument that the additional cost was required to deliver the pumps in time. Without this shipping cost, the production processes of IDES would have been affected. The second argument was that the particular shipping company was the only shipping company with available resources at the time. Team 1 was not able to collect any further evidence from the IDES system but suggested further steps of interrogating the shipping company and
tracing down the shipping documents. This shows that elaborate fraud cases require collecting evidence from all departments of an organization and not just the procure-to-pay process that we focus on in the WCHC.

In the third round, each team got the data sets of the other two teams for investigation. As illustrated in Table 3, only Team 3 was able to find sufficient evidence to definitively convict the other two teams. Team 1 and Team 2 were, however, able to provide evidence that the other teams were engaged in at least some aspect of the fraudulent behavior.

**DISCUSSION**

The WCHC is a novel teaching approach that allows students to experience the perspective and the behavior of a fraudster as well as what it means to investigate real-world enterprise information systems and to seek strong evidence as an interdisciplinary team of forensic investigators. In particular, walking in the shoes of a fraudster makes an impact on the understanding of forensic investigation, and sets the WCHC apart from other teaching approaches to forensic investigation (Brickner et al. 2010). Across the rounds, students gain a deeper understanding of fraudulent behaviors, fraud schemes, and activities necessary to camouflage the fraud itself. This provides the students with a more holistic understanding of the nature of fraud and helps the students to become better forensic investigators over the course of the WCHC (Digabriele 2008; Prabowo 2013).

The WCHC is also particularly useful to teach the limits of data analysis techniques. With each round the fraud cases become more elaborate and more ambiguous. As fraudsters, the participants think ahead and develop alternative explanations for their fraud schemes. The key to success in forensic investigation and thus in the WCHC is combining skills in accounting, security, and management with capabilities to investigate enterprise information systems to establish strong evidence even when facing highly ambiguous fraud cases (Digabriele 2008).
Naturally, the WCHC has some structural limitations. First, in our class experience of working with the IDES model company we found out that most of the model transactions raise red flags in the course of normal investigation. For example, investigating the bank account details of IDES employees and IDES creditors resulted in more than 300 matches (usually this is a red flag for false sales and shipping). However, we made students aware of this and of other similar shortcomings and suggested that this would be great opportunity to learn and try various forensic investigative methods. Second, the WCHC imposes a high load of self-organized learning and teamwork. Class instructors have to interact with the students regularly to identify problems and to clarify and direct the teams. One team, for example, spent considerable amounts of time focused on camouflaging techniques that turned out to be useless in the context of the IDES company, putting a heavy workload on the two instructors and one teaching assistant. Finally, the WCHC also creates a heavy load for the students. While self-organized teamwork helps the students to flexibly assign time to the contest, the contest setting requires students to put extra time into the course.

From a teaching perspective, the WCHC advertises forensic investigation as an attractive interdisciplinary field of study. Students learn to understand the behaviors of a fraudster, to acquire the capabilities to investigate enterprise information systems, and to seek particular evidence that contradicts statements put forward by suspects (Brody et al. 2012; Prabowo 2013). Furthermore, the WCHC answers the call for a more interdisciplinary perspective of teaching information security management (Hentea et al. 2006). Students have to combine knowledge from different disciplines to detect and to investigate potential fraud in ubiquitous information systems.

From a research perspective, the WCHC enables researchers to study the behavior of fraudsters in a laboratory environment that resembles a real-world environment. Usually, researchers are not able to observe fraudsters while they develop and commit their fraud schemes; rather, are only able to gather their data after the fact. The WCHC, however,
generates longitudinal data on how fraudsters interact with enterprise information systems as the students develop and test their fraud schemes. Hence, the WCHC serves as an intriguing starting point for field experiments in the domain of fraud detection, forensic investigation, and management controls (Abbasi et al. 2012; Pearson and Singleton 2008; Schermann et al. 2012).

CONCLUSION AND OUTLOOK

The WCHC is a novel approach to teach fraud detection and forensic investigation that is both attractive and appealing to students from different backgrounds. Future developments of this contest will include an online version to enable a larger number of students to participate. An online version of the WCHC will also allow us to include industry in sponsorship, participation, and judging of future iterations of the competition. In particular, the WCHC could be part of organizational information security awareness programs that help non-technical employees gain an understanding of security policies and management controls (Siponen 2000).

ACKNOWLEDGEMENTS

The authors acknowledge financial support from the Ernst Otto Fischer Teaching Awards from Technische Universität München. The authors would also like to thank Ingrid Prem and Manuel Wiesche for their invaluable assistance in making the white-collar hacking contest possible. The authors highly appreciate the support from KPMG and particularly thank Mirco Vedder and Michael Sauermann for their invaluable help.

REFERENCES


Association of Certified Fraud Examiners. 2012. “Report to the Nations on Occupational Fraud and Abuse,” Austin, TX, USA: Association of Certified Fraud Examiners, pp. 1–76.


