INTERNATIONAL JOURNAL OF GAMING HOSPITALITY TOURISM (IJGHT)
STOCKTON UNIVERSITY

Martin, A., Zaal, J., Azevedo, M., and Dutra, C. (2021). A Novel Decision Support Risk Assessment Tool for Investigating Internal Theft in a Gaming Establishment: A Case Study. *International Journal of Gaming Hospitality and Tourism.* 1(1). *https://stockton.edu/light/documents/ijght_vol.1-no.1/internal_theft_case_study_10.14.21.pdf*

A Novel Decision Support Risk Assessment Tool for Investigating Internal Theft in a Gaming Establishment: A Case Study

Alex Martin
Executive Operations
Clearspeed, San Diego, California, USA
alex.martin@clearspeed.com

John Zaal
Executive Operations
Clearspeed, San Diego, California, USA

Mario Azevedo
Call Center Services
Azevedo Solutions Group, Inc.
Kenwood, California, USA

Christine Dutra
Call Center Services
Azevedo Solutions Group, Inc.
Kenwood, California, USA

Acknowledgements:
The authors wish to thank (2) Dr. Leanne ten Brinke for her review of the manuscript. Her comments and suggestions helped improve and clarify the final version, (2) the Clearspeed R&D Department for their technical expertise and input on the project.

ABSTRACT
Employee fraud costs the average US gaming establishment with at least 1,000 workers roughly $3.3 million annually. Current internal theft identification strategies and methodologies are neither quick nor sufficient enough to curtail the financial damage, as it typically takes 12-16 months to detect and resolve most internal theft issues. The retrospective pilot case study described examines a novel artificial intelligence (AI)-enabled voice screening tool and its role in identifying previously undetected internal theft knowledge and involvement. In the total sample of 99 consenting study volunteers with no known history of internal theft, 0% initially admitted to a fraudulent offense. During the automated telephone interview, 3% of the entire subject pool provided a total of four admissions to either knowing about or being involved in internal theft. During the follow-up interview, 16.2% of risk-flagged participants made additional disclosures, germane to theft onsite. Previously undiscovered internal theft details were identified and confirmed. The 95.5% precise tool described can serve as a powerful addition to an organization's screening arsenal and aid in high-stakes issue prevalence estimates. Finally, this study's description of specific and predictive qualities of risk-positive employees contribute to the hospitality security and investigations literature.

Keywords:
casino investigations, decision support tool, internal theft, risk assessment

INTRODUCTION

Internal theft is one of the most covert and severe dangers to the survival of US-based institutions, costing businesses $20-50 billion a year. For each employee considered, businesses lose roughly $9 daily (Boss & Zajic, 2020). In particular within the U.S. gaming industry, for a property with 1,000 employees, loss due to occupational theft is $3.285 million annually (Association of Certified Fraud Examiners, 2020). Such a large financial burden reflects how challenging it is for casinos to maintain security when they are many things simultaneously: entertainment centers, hotels, restaurants, and governors of substantial cash (Strickhouser, 2004).

Considering the latter, it is alarming many casino properties spend more resources searching for external thieves than for the identification of internal threats (Association of Certified Fraud Examiners, 2020). Gaming executives sometimes equivocate whether adopting new investigative methodologies is worth the cost, especially for the detection of small internal theft (Bunn & Glynn, 2013). However, the literature is clear that without detection, losses only get dramatically worse and complex with time. Even in the most secure organizations, it is likely some type of employee fraud, inclusive of internal theft, will occur. Consequently, quick detection is vital to protecting an organization.

Internal Theft: Definitions and Examples

Depending on the situational context, internal theft may be referred to as fraud, pilferage, embezzlement, peculation, or defalcation, and can include one or more employees (e.g., collusion) (Purpura, 2020). Of the three primary categories of occupational fraud (i.e., corruption, financial statement fraud, asset misappropriation), the latter, which involves an employee stealing or misusing employer's resources, occurs in the vast majority (86%) of schemes (Association of Certified Fraud Examiners, 2020).

Examples of asset misappropriation abuses include theft of cash on hand, theft of cash receipts, fraudulent disbursements, misuse or theft of inventory, and larceny. The greater the number of perpetrators involved, the higher the loss, and longer the duration before being caught (Fennelly, 2016; Purpura, 2020) Whereas operational and human resource issues like recruitment, staffing, and retention have been well-recorded in the hospitality industry (Baum, 2002; Choi et al., 2000; Gustafson, 2002; Jameson, 2000), problems that involve internal theft have historically been underreported and under-researched (Kennedy, 2016; Pierce & Snyder, 2015). With respect to casino employee theft in particular, however, recent evidence demonstrates that: (1) the crime is committed secretly, (2) a control, policy, or procedure is violated or bypassed, (3) there is a paper (or electronic) trail, and (4) it happens every day, on every shift, in nearly every department (Boss & Zajic, 2020). In prior studies that have addressed it, internal theft has been appraised higher than sexual harassment as the most serious transgression of hospitality ethical standards (Poulston, 2008). Yet, despite its pervasive and costly nature to many hospitality operations, this employee-committed crime type is often underestimated, unnoticed, or ignored (Oliphant & Oliphant, 2001).

Historical Approaches Used by Casinos to Detect Internal Theft

For the gaming establishments that have sought to detect and control internal theft, there has not been a "one size fits all" approach. Different techniques have been used in various combinations, depending on resources (Boss & Zajic, 2020). These techniques include video and financial audits, tip-driven hotlines (as a result of human observations), security guard, and digital tool measures.

Some of the popular detection tactics, such as loss reporting through tip-driven hotlines, video audits, financial and compliance audits, and security guard protocols, have relied on human judgments (Boss &

Zajic, 2016; Purpura, 2020). Since it typically takes 12-16 months from the time internal theft begins to when it is reported or detected (Association of Certified Fraud Examiners, 2020), these approaches stand out for their operational weaknesses in not resolving issues quickly and early enough. Also, due to their reliance on subjectivity, these strategies are highly associated with bias and errors (Kemshall et al., 2011). Furthermore, sophisticated methods like money marking, detection sensors, GPS tracking chips, graph-based (data-mining) anomaly detection, and other digital tools can be problematic, since they are expensive and readily fooled by savvy employees familiar with security protocols. Even newer electronic detection analog systems (e.g., IP-based network cameras) have issues when the network goes down and the loss of real-time data and information occurs (Purpura, 2020).

Artificial Intelligence Approaches to Internal Theft

A more recent strategy US-based businesses have employed to detect employee theft is the implementation of artificial intelligence (AI) tools or "thinking machines". AI is defined as "the ability of a system to interpret external data correctly, learn from such data, and use these learnings to achieve certain goals and tasks through flexible adaptation" (Kaplan & Haenlein, 2019). The field of AI is relatively new, with milestones regarding its development since Turing's test in 1950 comprehensively described and summarized elsewhere (Buchanan, 2006; Brynjolfsson & McAfee, 2017; Kilichan & Yilmaz, 2020; Rigano, 2019.

For businesses seeking to counter theft and fraud in today's world, effective AI applications include automated financial patterns analysis and biometrics applications such as face recognition and voice detection. Compellingly, many machine learning systems have surpassed human-level performance in evaluating a person's cognitive state based on facial expression or voice outputs (Brynjolfsson & McAfee, 2017; Junoh et al., 2013; Rigano, 2019. As the banking industry has demonstrated, although 20 times more suspicious activity reports are generated compared to a decade ago, AI alerts produce fewer false positives (Quest et al., 2018).

AI has demonstrated its versatility and powerful ability to: (1) implement impartial predictive rules to recognize anomalies, (2) assess indicators of internal theft at an accuracy level that surpasses humans, and (3) be effective at saving time and money amidst large volumes of data (Bughin et al., 2017). Further, there is propitious evidence that AI applications provide new opportunities and competitive advantages to gaming and hospitality entities seeking to increase profit margins (Kilichan & Yilmaz, 2020, Zlatanov & Popesku, 2019). However, AI applications are still underutilized, with only 9% of U.S. businesses implementing it beyond experimental phases (Knight, 2020), and the travel and tourism industry as the sector with the lowest overall AI adoption index (Bughin et al., 2017). Notably in casinos, rather than being used for the detection of damaging, insidious crimes like internal theft, implemented AI-driven tools have been limited to external-facing applications (e.g., player fraud, curbside cheating; Thorson, 2020) and customer-centric functions (e.g., language translations, booking, check-in and check-out kiosks; Bisoi et al., 2020; Koranne, 2021). Particularly for casino operations seeking to identify internal theft, AI tools could complement existing risk assessment strategies.

The Present Case Study

As a result of discovering a substantial internal theft crime in their organization the prior year that involved several floor-level employees and over $1 million in financial losses, the gaming industry executives who approved the pilot acknowledged the gap in their detection strategies and were highly motivated to evaluate and potentially implement a new AI-driven approach. Their use case was chosen for retrospective analysis as (1) the environment and population reflected the real-life conditions wherein the tool was designed to be used, (2) the sample size afforded high statistical power, (3) multiple variables were available for analysis, and (4) verification was available for flagged results.

The primary purpose of this study was to explore the value of a novel AI-driven automated technology as a fast, objective, and precise flagging tool of internal theft knowledge or involvement, when implemented in a gaming organization's chain of risk assessment screening steps with employees. Specifically, the automated technology identifies vocal signals in response to simple yes/no responses to high-stakes questions about knowledge or involvement in internal theft. These signals are combined to produce a risk assessment metric - 'flagging' cases for follow-up interviews. The secondary purpose was to contribute to the existing literature by providing details about trends linked to risk results, such that security and management personnel can be better equipped in their investigation efforts.

Derived from the primary study purpose, the following hypotheses were tested: H1a: The automated technology would produce variation in risk assessment outputs; H1b: The flagging performance of the automated technology would be precise, H1c: No individual question would outperform the others, H1d: The perception of stakes would be directly correlated with risk-positive results, H1e: The perception of stakes would be inversely correlated with the number of admissions made, and H1f: The automated technology would classify admissions as risk-negative responses. Derived from the secondary study purpose, the following hypotheses were tested: H2a: Risk-positive interview outcomes would be positively predicted by job tenure, H2b: Risk-positive interview outcomes would be positively associated with audible tell categories, H2c: Audible tells in risk-positive interviewees would not be affected by gender, and H2d: Interview outcomes would not be predicted by gender, self-reported anxiety, shift work, or interview date.

METHODS

In this pilot study, wherein we investigate the promise of a novel AI tool in the detection of internal theft, the retrospective use-case approach is featured. Anchored in ecological validity, wherein critical events and interventions can be examined in detail and in real-life context, the case study approach is an applied research methodology that results in a multi-faceted and holistic account of the observations under study. Considering the frequency with which innovation applications are taking place in our society and how well the case study approach lends itself to answering in-depth questions, it was appropriate to adopt this design (Flyvbjerg, 2006; Gray, 2018; Hamel et al., 1993; Robson & McCartan, 2016).

Participants

To address whether one sample of a west-coast, non-tribal gaming establishment's floor-based employees had ever known about or participated in an act of internal (employee) theft, and to assess the utility of the automated tool, data originated from study volunteers included the majority of bankers and dealers of the company's largest standalone flagship location (i.e., 6.4% of the gaming establishment's total employees). Based on the aforementioned evidence linking floor employees to the prior large-scale theft the gaming establishment experienced, and the fact bankers and dealers had the most proximate and consistent access to chips and/or cash, only floor-level personnel were asked to participate in the pilot. No on-site criminal activity associated with specific employees who participated in the pilot was known to the management team, prior to and during the time period the automated interviews were scheduled, given, and followed-up. Although none of the n=100 study volunteers underwent attrition (e.g., due refusal to participate, medical or mental faculty reasons, etc.), one interview was never executed (due to participant anxiety) and three were only partially completed (due to instructional disregard). Of the n=32 employees who produced the highest risk results and were scheduled to meet with the interviewing expert, n=10 did not complete the follow-up interview (e.g., due to having called in sick, not having been available, etc.). For this analysis, we included all employees who completed the screening procedure and had no exclusionary conditions; therefore, the final sample consisted of n=96 fully completed automated interviews, n=3 partially completed automated interviews, and n=22 followed-up interviews.

For each of the *n*=96 fully and *n*=3 partially completed interviews, the participant voluntarily consented to taking the automated interview as part of a pilot study of the tool for the use-case of thematic offenses associated with internal theft. As concerns the total study sample and relevant interviews, the following was discerned: males represented 79.8% of the participants, with females comprising the remaining 20.2%; 39.5% worked the day shift (6 AM to 2 PM), 40.4% worked the night shift (2-10 PM), 6.1% worked the graveyard shift (10 PM to 6 AM), and 14.1% worked on a shift that was not recorded; 3.0% reported having recently experienced a traumatic event; 0% had consumed alcohol or drugs that day; and 0% had experienced illness or pain that day. Of the *n*=22 flagged personnel who were followed-up on, the average amount of time each had been employed at the gaming establishment was 34.36 months (*SEM* = 5.46).

Design

When testing most hypotheses, the pertinent questions (PQs**;** independent variables) posed by the automated tool were the stimuli. Other than tool-generated risk outputs (dependent variables), the additional descriptive data collected (e.g., gender, shift worked, tenure, interview dates, audible tells) and self-reported details (i.e., recent trauma, alcohol/drug consumption, illness, pain) were extraneous variables. Additional factors used in analyses were admissions of either knowing or being involved in internal theft, and confirmatory details discerned by the independent follow-up expert and fact-checked prior to being used for verification of flags.

Automated Interview Foci

The interview approaches and PQs were the same for all employees who participated in the pilot study. To minimize threats to validity, only the most salient, highest-stakes issues were addressed, reflected in the limited number (i.e., six) PQs approved in writing by the client management team. These questions were based on a combinatorial approach of expertise and in-depth communications with the client's executive team, regarding the history, perceived pervasiveness, and impact of internal theft, fraud, embezzlement, and collusion at their establishment. In each interview, the actual name of the client was referenced. However, for the purpose of retaining anonymity, in this paper, the client's name has been replaced by the term "gaming establishment" (Table 1).

Table 1: Pertinent Questions used in "Gaming Establishment" Pilot Study of Risk Analysis Tool

1. Do you know the identity of any employee cheating or in any way purposely altering the outcome of a game?
2. Do you know the identity of any casino or "gaming establishment" employee stealing from a "gaming establishment" or casino?
3. In the past year, has anyone asked for your help in stealing from a "gaming establishment" or a casino?
4. Have you purposely allowed anyone to receive chips they did not legitimately pay for or win?
5. In the past year, have you taken anything worth more than $25 that belonged to a "gaming establishment" employee without their approval?
6. In the past year, have you taken anything worth more than $25 that belonged to a "gaming establishment" or a casino without approval?

Apparatus

Investigative Tool

Clearspeed Verbal, henceforth referred to as "the automated technology", is an enterprise-level, scalable voice analytics tool that quickly assesses an individual's risk association relative to explicit themes or

issues by means of an automated telephone interview. By evaluating specific vocal articulation outputs, this automated system detects and quantifies the presence or absence of voice-based risk reactions to client-defined questions. The AI-enabled technology leverages validated voice analytics and technical processes to evaluate responses to specific questions asked during the interview.

Unique Aspects of the Technology

The automated technology enables precise risk alerts based on an individual's vocal responses in any language, without the need to store personal identifiable information (PII). The tool incorporates the use of issue-specific questions asked during an automated telephonic interview to evaluate the presence or absence of risk signatures in the voice. Researchers have provided evidence that perceptions and cognitions are communicated through the voice (Cowen et al, 2019; Simon-Thomas et al., 2009). In the automated process, the voice characteristics evaluated are the result of distinct neurocognitive reactions to specific screening questions and have neural correlates (Dedovic et al., 2009; Farrow et al., 2013; Muehlhan et al., 2013). There is ample evidence that specific information in human voice outputs can indicate the presence or absence, and intensity, of Central Nervous System and Autonomic Nervous System driven reactions in real-world environments wherein the perception of high-stakes is involved (e.g., Brenner et al., 1994; Laukka et al., 2008; Ruiz et al., 1990; Scherer, 2003; Sondhi et al., 2015; Van Puyvelde et al., 2018; Williams & Stevens, 1972). Further, the link between linguistics, vocal cues, and risk markers of fraud detection has been established (Throckmorton et al., 2015). The automated technology described here creates a model of the human voice in any language, for "yes" or "no" responses to risk-focused questions. The voice model is transformed, processed, analyzed, and quantified using a series of proprietary methodologies which evaluate and classify specific features of vocal responses. Once the voice input completes the processing cycle, a risk level for each response to specific questions is calculated and assigned, from low-to-high.

Technical Process

The automated telephonic interview process employs Session Initiation Protocol (SIP) capable of securely conducting hundreds of simultaneous telephonic interviews from anywhere in the world. Therefore, the main requirement to use the technology is a stable telephone connection (landline or cellular). Upon interview completion, an encryption system packages the user responses, which are securely transferred to an AI-driven risk evaluation system, trained via supervised-learning using labeled data. Additionally, multiple Quality Control processes are used to ensure the precision and accuracy of each evaluated response. A report of the evaluation is then automatically created and transferred to the client in the desired format. All data are encrypted both at rest and in transit. Interview results are typically accessed via a secure online dashboard, based on user role and permissions (i.e., the account owner can control and define permissions and restrict information only to those who need to see/use it). The expected turnaround time for results is within 24-hours of interview completion.

Continuum of Individual Responses and Overall Results

The automated technology's risk framework boundaries are established (i.e., remain constant), wherein evaluation output results fall into one of four risk determinations along a continuum: low risk (LR) which equates to no risk, average risk (AR) which equates to negligible risk, potential risk (PR), which equate to a mid-level of risk, and high risk (HR). In this particular evaluation, due to the six PQs asked, each interview produced a total of six risk-reaction results, with one of four AI-generated risk scores per question. The highest risk score among all questions determined the overall risk assessment.

Interview Outcome Categories

Following the automated process, each interview was associated with an outcome result along a continuum: low risk (LR), average risk (AR), potential risk (PR), and high risk (HR). Further, three

additional outcomes are: admission (AD), suspected countermeasure (CM), and not completed (NC). The latter three results are the result of QC evaluation and scoring. An admission (AD) was the effect of a "yes" response to any PQ asked. A CM was the result of an interviewee showcasing specific behavioral characteristics (e.g., inaudible whispers to all questions), described elsewhere (Hughes, 2017; Navarro & Karlins, 2008; Nierenberg, 2010. An NC interview was the result of technical or similar issue (e.g., bad telephone connection) occurring during the interview. Risk-negative interviews were those in the LR and AR ranges. Risk-positive interviews with outcomes of PR, HR, AD, or CM are typically recommended for follow-up.

PROCEDURE

For all personnel at the gaming establishment who voluntarily participated in the pilot-study described, the screening process consisted of four to five distinct phases that transpired during the three shifts of each of the five pilot-study days: (1) the initial announcement, (2) the pretest introduction, (3) the pretest interview, (4) the automated interview, and (5) the follow-up interviewee (for risk-positive interviews). The interview process phases are described next and also highlighted in Figure 1. It should be noted that steps 2-5 showcased in Figure 1 mirror the standard operating procedure of the described automated technology.

Figure 1: Steps of Interview Process

SAME DAY

Daily Pre-shift Meeting

(Step 1: Initial Announcement)

- Shift leader informed employees that floor personnel volunteers will participate in pilot-test study to test tool
- Schedule & logistics provided

Interview Room

(Step 2: Pretest introduction)

- Upon entering room, employee employee given instructions and list of pertinent questions
- Manager dialed center, input code, handed phone to employee, and left room

Interview Room

(Step 3: Pretest interview)

- Call center agent:
  - asked prescreening questions
  - informed employee of what to expect
  - requested consent

Interview Room

(Step 4: Automated interview)

- Automated voice reiterated instructions.
- Two to three iterations of same questions asked

DIFFERENT DAY

Private Room

(Step 5: Follow-up interview)

- Employees with risk positive results followed-up by expert
- Explanations for flags on questions were explored within a 30-minute time frame

Interview Phases

Initial Announcement

At each pre-shift meeting, the shift leader orally announced to all meeting attendees that as part of a pilot evaluation of a new screening tool, site-based personnel would be asked to voluntarily participate in an automated telephone interview that day. Logistical details were then provided (i.e., scheduled time and location of the interview).

Pretest Introduction

At their allotted time, the participating employee entered the designated room, a clean and neutral private office, furnished with a desk and telephone. After requesting that the employee sit at the desk with the telephone, the location manager (previously trained to supervise and administer the interviews) informed of general instructions, including the need to answer all questions accurately. For clarity and transparency, the manager then provided the employee with a list (to read) of the interview questions that would be asked, and informed about the importance of only answering "yes" or "no" to each. After successfully dialing a call center and introducing a unique code that deidentified the interviewee, the manager handed the phone to the employee and stepped out of the room.

Pretest Interview

At this point, over the telephone, a call center agent asked the following short list of prescreening questions germane to the employee's ability to successfully complete the interview: Have you taken any drugs today? Have you consumed any alcohol today? Are you experiencing any illness or pain? and Have you recently experienced a major traumatic event? Based on the agent's observations as to any prescreening flags, a decision was made as to whether the employee could proceed with the process. If so, the agent informed the employee that (1) upon initiation of the automated portion of the call, they would hear a set of instructions, (2) that several iterations of the same question set was typical, and (3) the agent would remain on the line, in case any technical problems ensued. The next step was initiated only after voluntary consent to take the interview and have it recorded was obtained.

Automated Interview

Upon the initiation of the interview, an automated voice informed each employee that they would be asked several direct questions requiring accurate responses. Two iterations of questions were asked to ensure the quality of the captured responses. When the interview was completed, the employee hung up the phone, left the room, and returned to work. From initiation to completion of the call, the automated interview averaged less than ten minutes.

Posttest Follow-up Interview

Only for volunteers who produced the most serious risk-positive flags (i.e., HR, AD, and/or CM on at least one question), a follow-up interview based on an established methodological approach (Hughes, 2017) was conducted four to six weeks later by a behavioral expert consultant. During each follow-up interview (the basis for establishing ground truth), explanations for flags on particular knowledge and/or involvement-based questions were thoroughly explored within a 30-minute time frame.

Systematic Approach

The gaming establishment's project team for the described pilot study consisted of the Chief Operating Officer, location manager, and security manager. The project team enabled methodological consistency, in that all automated interviews were administered on the same day floor personnel voluntarily agreed to participate in the pilot. Of the five work days whereby automated interviews were implemented, 20.2% occurred on Day 1 (April 12, 2019), 8.1% occurred on Day 2 (April 13, 2019), 19.2% occurred on Day 3

(April 16, 2019), 30.3% occurred on Day 4 (April 18, 2019), and 22.2% occurred on Day 5 (May 8, 2019). All interviews were scheduled and taken within 2.5-4 hours of each shift's start (i.e., average times of 10:28 AM, 6:00 PM, and 12:33 AM for the day, night, and graveyard shifts, respectively). All follow-up interviews were conducted onsite during a three-day period in early June, 2019. The total number of *n*=99 partially and fully completed automated interviews consisted of the majority (92.9%) having only required two iterations of questions versus the minority (7.1%) having required three. A third iteration of questions was only required when the system detected quality issues in responses during the prior iterations.

Statistical Tests

The following analyses were executed via IBM SPSS Statistics 23 software: the non-parametric Chi-Square Goodness of Fit Test, the rank-based Friedman analysis of variance, the non-parametric rank correlation Spearman's test, cumulative odds ordinal logistic regression, and multiple regression. Additionally, the following analyses were executed via Microsoft Office Excel 2016 software: frequencies of AD risk score outcomes, Student's t-test, and positive predictive value (PPV) proportion tests. *NOTE: When evaluating PPVs, the following definitions applied: "not confirmed" meant justification for the risk-positive score was not found, "confirmed" meant justification for the risk-positive score was found, "confirmed-validated" meant verification of risk or admission was due to factually- confirmed knowledge and/or involvement, and "confirmed-mitigated" meant verifications of the risk-positive reaction resulted from associative memories, confusion (e.g., language barrier), or anger at management (i.e., deliberate attempts to manipulate results).*

Ethical Standards

All procedures followed ethical standards of the responsible committee on human experimentation [institutional and national] and the Helsinki Declaration of 1975, as revised in 2000. Not originally collected for research purposes, the data represented real-world research. Participants' privacies were respected and protected according to established ethical guidelines (Robson & McCartan, 2016), with personally identifiable information either anonymized, kept confidential, or not collected at all.

RESULTS

Descriptive Statistics

Individual Response Risk Results

The study of *n*=96 completed and *n*=3 partial interviews resulted in a total of n=622 evaluated responses (i.e., LR, AR, PR, HR, AD, CM, NC). Some questions elicited additional response information based on the automated evaluation and quality control review (e.g., AD and CM). Of the *n*=617 detected responses, the PQ risk evaluation frequencies distributed as follows: 43.9% (*n* =271) LR; 26.1% (*n* =161) AR; 19.1% (*n* =118) PR; 6.3% (*n* =39) HR; 0.6% (*n* =4) AD; and 3.9% (*n* =24) CM (Table 2).

Interview Outcome Results

Of the *n*=96 fully completed interviews, the overall interview assessment outcomes distributed as follows: 9.4% (*n*=9) LR; 14.6% (*n*=14) AR; 43.8% (*n*=42) PR; 25.0% (*n*=24) HR; 3.1% (*n*=3) AD; and 4.2% (*n*=4) CM (Table 2).

Table 2: Comparison of result type frequencies of individual responses and interviews

Evaluated risk	Individual responses (n = 617)	Interview outcomes (n = 96)
Low Risk (LR)	43.9% (n = 271)	9.4% (n = 9)
Average Risk (AR)	26.1% (n = 161)	14.6% (n = 14)
Potential Risk (PR)	19.1% (n = 118)	43.8% (n = 42)
High Risk (HR)	6.3% (n = 39)	25.0% (n = 24)
Admission (AD)	0.6% (n = 4)	3.1% (n = 3)
Countermeasure (CM)	3.9% (n = 24)	4.1% (n = 4)

Pertinent Question Risk Results

PQ6 elicited the highest number of HR responses (35.9%). PQ5 elicited the highest number of PR responses (25.4%). Although each interview consisted of equal numbers of "knowledge" (PQs 1-3) and "involvement" (PQs 4-6) questions, the more consequential "involvement-theme" questions produced the greatest number of HR and PR responses.

Audible Indicator Results

A portion (38.3%) of the automated interviews described were accompanied by n=22 distinct and perceptible alert indicators of speech or audible "tells" (Collett, 2004; Hughes, 2017) that were observed and noted by seasoned call center agents, Of n=38 interviews, the following single tell displays (and respective frequencies) were revealed in n=25 interviews: repeat replies (2.63%), whispers (2.63%), reply changes (10.53%), yeah vs. yes responses (5.26%), vocal hesitations (7.89%), pitch changes (7.89%), laughter (2.63%), nose clearing (2.63%), tone differences (7.89%), speed changes (2.63%), not responding (2.63%), stuttering (2.63%), answering as a question (2.63%), and surprise (2.63%), and responding "no" to all neutral questions (2.63%). In n=13 of the remaining interviews whereby audible tells were noted, the following combinatorial tell displays were each represented once (each at 2.63%): pitch changes/response delays, interjection (uhs)/premature response, yawning/laughing, coughing/response delays, grunting/response delays, reply changes/response delays, not responding/repeat replies, yawning/tone differences, yeah vs. yes responses/response delays, repeat replies/throat clearing, interjection (uhs)/reply changes, yeah vs. yes responses/reply changes, pitch changes, and interjection (uhs)/yeah vs. yes responses/response delays.

Inferential Statistics

Observed vs. Expected Interview Response Frequencies

To test H1a, we conducted a Chi-Square Goodness of Fit test. Of the n=96 fully completed interviews, n=89 participants completed interviews consisting of n=534 responses that were "purely" assessed as LR, AR, PR, or HR (as a result of "yes" or "no" responses to the six questions relevant to casino theft). The statistical test revealed the assessments distributed unequally across the different risk levels. Specifically, low risk evaluations were most common, $\chi 2$ (3, N = 534) = 181.236, $p < 0.00001$.

Flagging Precision

To test H1b, we executed a positive predictive value analysis. Whereas four ADs among three employees were made during the actual automated interview, all disclosure details were solely provided during the in-person posttest follow-up, when 16.2% of the subject pool made ADs relative to theft onsite. Of the n=32 volunteers whose automated interviews flagged highest for risk (i.e., n=25 HR, n=4 CM, n=3 AD),

n=22 of them were followed up by an independent third-party expert. Of these, *n*=1 was not confirmed (i.e., was a potential Type I error). However, of the *n*=21 who confirmed, 76.2% (*n*=16) were confirmed-validated, and 23.8% (*n*=5) were confirmed-mitigated. Therefore, the automated output and results production process showcased a high positive predictive value (PPV) of 95.5%.

Differences in Pertinent Questions

Application of the Friedman test revealed no evidence of stochastic dominance between the PQs for score outputs, $\chi 2(5) = 5.895$, $p = .317$. Consistent with H1c, then, there was no evidence that any individual question outperformed the others.

Relationship Between Perceived Stakes and Risk Outputs

The rank order of perceived question consequence was PQ6 > PQ5 > PQ4 > PQ3 > PQ2 > PQ1. Taking into account the results of *n*=534 individual risk responses from *n*=89 completed interviews (excluding ADs and CMs), a Spearman's rank correlation test produced a scatterplot, that visually revealed a monotonic relationship, $r_s(6) = 0.812$, $p = 0.05$. Consistent with H1d, a strong direct (positive) and significant correlation existed between perceived question stakes and risk-positive results.

Relationship Between Perceived Stakes and Admissions

In addition to the aforementioned rank order of perceived question consequence, the rank order of AD number by PQs was determined to be: PQ1 > PQ3 > (PQ2 = PQ4 = PQ5 = PQ6 = 0). Of all four ADs made, 100% were associated with knowledge-themed (lower consequence) questions. Considering the results of *n*=4 AD risk responses from *n*=3 interviews, a Spearman's rank correlation test produced a scatterplot, that visually revealed a monotonic relationship, $r_s(6) = -0.676$, $p = 0.140$. In support of H1e, a strong, negative correlation was found between perceived question stakes and ADs. However, this relationship was not significant.

Relationship Between Admissions and Risk Outputs

3.03% (*n*=3) of a total 99 interviews resulted in ADs during the automated interview phase. With *n*=4 ADs among *n*=3 admitters, the average rate was 1.3 admissions/admitter. Of all *n*=4 AD responses made in this particular pilot, 75% (*n*=3) were associated with LR, and 25% (*n*=1) was associated with AR evaluations. Therefore, 100% of ADs made during the automated interview were associated with risk-negative results, which supports H1f.

Feature Relationship Analyses

Relationship Between Tenure and Confirmed Risk Positive Outcomes

To test H2a, an ordinal logistic regression analysis included the *n*=21 (HR, AD, CM) flagged interviews that were confirmed. The assumption of proportional odds was met, as assessed by a full likelihood ratio test comparing the fit of the proportional odds location model to a model with varying location parameters, $\chi 2(4) = 1.256$, $p = .869$. The deviance goodness-of-fit test indicated that the model was a good fit to the observed data, $\chi 2(26) = 14.918$, $p = .959$. The Pearson goodness-of-fit test indicated that the model was not a good fit to the observed data, $\chi 2(26) = 22.575$, $p = .657$. The final model statistically significantly predicted the dependent variable over and above the intercept-only model, $\chi 2(4) = 9.138$, $p = 0.05$. It was determined the longer period of time a flagged employee was on their job at a gaming establishment, the higher the odds were they would produce a risk reaction for both "knowledge" and "involvement" questions, with an odds ratio of 1.084, 95% CI [1.002-1.173], Wald $\chi 2(1) = 4.008$, $p = .045$. However, there were no significant effects of gender and shifts worked on the complexity of risk involvement.

Relationship Between Interview Outcomes and Speech Indicator Categories

To test H2b, the results of *n*=96 completed interviews and *n*=22 audible "tell" categories were considered. A Spearman's test revealed a monotonic and significant positive correlation between the risk outcome of an interview and the number of audible tell categories identified by human call center operators, $r_s(94) = 0.23$, $p = 0.024$. Notably, this correlation is considered small by conventional standards (Cohen, 2009), and indicates that human vocal evaluation cannot replicate what is captured by AI.

Predictors of Speech Indicator Quantity

Further, to test H2c, with respect to regression analysis, linearity was assessed by partial regression plots and a plot of studentized residuals against the predicted values. Residuals were independent, as assessed by a Durbin-Watson statistic of 1.843. There was homoscedasticity, via visual inspection of a plot of studentized residuals versus unstandardized predicted values. There was no evidence of multicollinearity, as assessed by tolerance values greater than 0.1 and Cook's distance values above 1. The assumption of normality was met, as assessed by a Q-Q Plot. The multiple regression model significantly predicted audible cues, $F(9,93) = 4.908$, $p = .001$. Specifically, female employees' risk-positive interview outcomes predicted a greater number of audible behavioral tells, as showcased and observed from speech. (Table 3).

Table 3: Prediction of Audible Speech Tells

Summary of Multiple Regression Analysis

Variable	*B*	SE_B	*β*
Intercept	-0.024	0.800	
Gender	-0.634	0.397	-0.087*
Interview Risk Outcome	0.906	0.235	0.371**

Note. *p < 0.05, **p < 0.01; *B* = unstandardized regression coefficient; SE_B = Standard error of the coefficient; β = standardized coefficent

Interview Outcome Predictors

To test H2d, an ordinal logistic regression analysis was conducted that included the *n*=96 completed interviews. The assumption of proportional odds was met, as assessed by a full likelihood ratio test comparing the fit of the proportional odds location model to a model with varying location parameters, $\chi2(32) = 9.429$, $p = .99$. The deviance goodness-of-fit indicated that the model was a good fit to the observed data, $\chi2(77) = 70.452$, $p = .688$. The Pearson goodness-of-fit indicated that the model was a good fit to the observed data, $\chi2(77) = 74.803$, $p = .550$. The final model showed that gender, self-reported anxiety, shift worked, and interview date did not statistically significantly predict the dependent variable over and above the intercept-only model, $\chi2(8) = 8.234$, $p = 0.411$.

DISCUSSION

In this retrospective pilot use-case study in a US gaming establishment, a novel, automated tool effectively and precisely alerted the client to risk identifications of information and employees knowing about or being involved in internal theft. Since the unique data originated from one organization and one independent (third-party) expert conducted the follow-up interviews, fewer potentially confounding variables were introduced (e.g., differences in training styles, procedures, and timings of interview execution).

Notable Findings

Indicative of the tool's precision, it was 95.5% probable that a flag would be confirmed in a follow-up interview. This result is consistent with the >94% PPV the technology consistently achieved in similar

historical operational (commercial and military) testing settings wherein verification details of follow-up interviews were available (data not shown).

Despite a few instances when participants misunderstood questions (due to language barriers), the pertinent queries were found to be equally effective in predicting risk, reflective of the effective collaboration between the client and operational personnel re question development. Further, volunteers' perceptions of the stakes intrinsic to each question directly and significantly correlated with flagged reactions. This finding is substantiated by the literature, which demonstrates that when questions are perceived as high stakes, vocal signals that are easier to discern, more robust and more reliable than those derived in the lab (Brenner et al., 1994; Mendoza & Carballo, 1998; Ruiz et al., 1990).

With respect to admissions, after each employee was queried about their ties to internal theft, they had the opportunity to reveal critical information. None disclosed information prior to the introduction of the process. In all cases, the first admission happened either during or after execution of the automated interview. Although it was found that the more an interviewee perceived stakes in queries, the less likely they would provide disclosures, this trend was not statistically significant, which may have reflected the weak sample power (i.e., more than n=4 admissions may have produced a significant effect). Despite the latter, it is notable that 100% of the admissions were associated with the absence of risk detected in voice outputs (i.e., no detectable reactions). This trend is not new. When averaging prior operational data spanning twenty similar projects (n=372 admissions, n=18,763 non-admissions), disclosures were consistently and significantly associated with higher risk-negative and lower risk-positive vocal output frequencies than their non-admission counterparts (data not shown). These findings corroborate the literature that disclosures serve as points of release, expressed in attenuated, acute alert reactions (Farrow et al., 2013; Suchotzki et al., 2017; Verschuere et al., 2018).

As predicted, it was determined that the longer a person's employment tenure was at the gaming establishment, the greater the chances they would flag on both knowledge and involvement questions (i.e., increased and more complex associations with internal theft issues queried). This finding corroborates the literature, that the longer a thief has worked for an organization, the higher and more complicated the losses and crime ties tend to be (Boss & Zajic, 2020) and the more prone he is to risk-knowledge and involvement associations. However, since the literature additionally demonstrates that employees with more authority can also be associated with asset losses (Boss & Zajic, 2020), it behooves the most prudent of gaming security teams to conduct risk assessments on employees within all positions and departments. It was additionally discerned that risk-positive interviewees were observed to engage in more speech-tells. However, counter to what we predicted, female risk-positive interviewees elicited more speech tells than their male counterparts did. Although significant, this relationship was shown to be weak, corroborating the literature that verbal alert response cues that solely rely on human perception are often unreliable (Johnstone & Scherer, 2000; Laukka et al., 2008). In other words, being attentive to the behavioral signs of a risk-assessed employee may be helpful in guiding the investigative heavy-lifting needed to produce an admission in a high-stakes area. However, since human judgement is wrought with subjectivity and bias, paying greater attention to objective AI-based risk-alerts is prudent (Kleinberg & Verschuere, 2021).

Finally, despite evidence that most employees who commit internal theft in US gaming establishments are first-time offenders and male (Association of Certified Fraud Examiners, 2020), in this study, interview outcomes (and risk complexity) were not impacted by gender, pre-existing anxiety, shifts worked, or dates of execution. It was particularly paramount to rule out gender bias; companies that implement decision support screening tools like the one described don't want to find themselves in situations where systemic bias towards specific types of employees for dubious activity are propagated (Feast, 2019).

Limitations and Future Research

Due to the necessary ethical constraints on personal information collected (Robson & McCartan, 2016), specific characteristics of the client's establishment and employees (e.g., age, race, criminal history, socioeconomic strata, and education level) were not be explored, which could have further enriched the analyses.

A further study disadvantage was the potential for design compromise, if and when participants divulged interview details (e.g., the process, questions) with each other. Distinguishing between study naïve and informed participants could have facilitated further statistical modeling. Additionally, consistent environmental control of interviews for noise was not rigorously implemented, as reflected in the three instances of background noise having been detected while automated interviews were conducted. The conspicuously low frequency (4.5%) of potential false positives may have reflected the objective nature of the automated technology, the prevalence of risk in the population sampled, and/or the skills of the follow-up expert. Nevertheless, even a low frequency of false positives can be associated with issues for an organization that adopts a novel risk management strategy. The consequences of making a Type I error can equate to an intervention that is unnecessary, and thus a waste of resources. Further, repeated overestimations of risk can, over time, tarnish the reputation of an organization. If an automated screening tool is deployed from a disciplinary human resource perspective, the privileges and status of employees who produce flagged interviews may be compromised up to the point of and after they are cleared (Kaminski & Schonert, 2017; Kemshall et al., 2011; Murphy et al., 2014)

A screening metrics constraint of this study was the inability to confirm risk-negative results (i.e., true vs. false negatives). However, as is usually the case with field studies of real-world research, the implementation of known positives and known negatives (in control vs. experimental groups) was not a viable option.

Finally, although the use of AI-driven systems holds great promise to boost profitability, productivity, and morale in gaming organizations seeking enhanced risk identification strategies, there are also potential ethical concerns to consider, including (1) machines replacing humans in jobs devoted to risk detection, (2) lack of transparency of technological complexity and issues like concept drift, and (3) integration challenges with existing organizational risk management protocols and tools. (Chui & Manyika, 2018; NI Business Info, 2020). Future studies that address the latter ethical points would be beneficial to the field.

CONCLUSIONS

One of the implications of this study is that AI-enabled automated technologies like the one described can serve as powerful investigative additions to the screening tool arsenal already in place for gaming establishments. Resilient organizations value of complementary risk assessment strategies that assess signals, along a continuum from low-to-high, such that actionable steps can be taken to identify, mitigate, isolate, monitor, avoid, transfer, or escalate flagged issues (Gius et al, 2018, Meyer et al, 2011; Tselyutinaet al., 2020). The most rigorous of correctly implemented and contemporary interdisciplinary risk assessment systems are continuous, holistic, layered, redundant, technology-enabled, interdisciplinary, and serve the purpose of helping end-users identify risk in order to make better decisions faster, while allocating their precious resources accordingly (Gius et al, 2018).

Another implication is that the automated tool can help gaming security managers gain realistic insights about the prevalence of high-stakes issues in their establishments, such that resources are suitably allocated. In the pilot described, the client's security team discerned that floor-level employees connected to internal theft were more prevalent than previously estimated.

We underscore that in guiding gaming organizations where to focus resources, the automated tool described only distinguishes between risk-positive and risk-negative voice responses; it does not expose the rationale behind the signals. Since even the best AI-assessment tools can't make absolute determinations of "risk" or "liability", in screening situations, they identify, not adjudicate. Therefore, the results derived should not exclusively be used as "evidence" in employee terminations or legal cases. The neurocognitive reactions that affect vocal outputs (translated into risk) can be due to a variety of reasons other than malfeasance (e.g., auxiliary memories, associations, and individual variability). The follow-up team of investigative experts should ascertain what the resultant risk flags mean. Whereas machines can provide risk-reaction flags, decisions on how to interpret and proceed with these alerts must be deferred to humans, who comprehend nuances.

REFERENCES

Association of Certified Fraud Examiners. (2020). (rep.). *Report to the Nations 2020 Global Study on Occupational Fraud and Abuse.* https://www.acfe.com/report-to-the nations/2020/

Baum, T. (2002). Skills and training for the hospitality sector: a review of issues. *Journal of Vocational Education & Training*, *54*(3), 343–364. https://doi.org/10.1080/13636820200200204

Bisoi, S., Roy., M., & Samal, A. (2020). Impact of Artificial Intelligence in the Hospitality Industry. *International Journal of Advanced Science and Technology*, *29(*5), 4265-4276. https://www.researchgate.net/publication/343180745

Boss, D. J., & Zajic, A. W. (2016). *Casino Security and Gaming Surveillance*. CRC Press.
Boss, D. J., & Zajic, A. W. (2020). Employee Theft Investigations. In *Casino and gaming resort investigations* (pp. 110–124). essay, Routledge.

Brenner, M., Doherty E. T., & Shipp T. (1994). Speech measures indicating workload demand. *Aviation, Space, and Environmental Medicine*, *65*, 21-26. https://psycnet.apa.org/record/1994-20587-001

Brynjolfsson, E., & McAfee, A. (2017, July 18). The Business of Artificial Intelligence. *Harvard Business Review*. https://hbr.org/2017/07/the-business-of-artificial-intelligence

Buchanan, B. G. (2006). A (very) brief history of artificial intelligence. *AI Magazine*, *26*(4), 53-60. https://doi.org/10.1609/aimag.v26i4.1848

Bughin, J., Hazan, E., Ramaswamy, S., Chui, M., Allas, T., Dahlstrom, P., Henke, N., & Trench, M. 2017). *Artificial Intelligence: The next digital frontier?* (Rep. No. Discussion Paper, June 2017). McKinsey & Company. https://www.mckinsey.com/~/media/mckinsey/industries/advanced%20electronics/our%20insights/how%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/mgi-artificial-intelligence-discussion-paper.ashx

Bunn, M., & Glynn, K. M. (2013). Preventing Insider Theft: Lessons from the Casino and Pharmaceutical Industries. *Journal of Nuclear Materials Management*, *41*(3), 4-16. http://nrs.harvard.edu/urn-3:HUL.InstRepos:10861136

Choi, J. G., Woods, R. H., & Murrman, S. K. (2000). International labour markets and the migration of labour forces as an alternative solution for labour shortages in the hospitality industry. *International*

Journal of Contemporary Hospitality Management, *12*(1), 61-67. https://doi.org/10.1108/09596110010305154

Chui, M., & Manyika, J. (Hosts). (2018, April 25). *The real-world potential and limitations of artificial intelligence* [Audio podcast with David Schwartz]. McKinsey & Company. https://www.mckinsey.com/featured-insights/artificial-intelligence/the-real-world-potential-and-limitations-of-artificial-intelligence

Cohen, J. (2009). *Statistical power analysis for the behavioral sciences*: Psychology Press.

Collett, P. (2004). *Book of Tells*. Transworld Publishers Ltd.

Cowen, A. S., Elfenbein, H. A., Laukka, P., & Keltner, D. (2019). Mapping 24 emotions conveyed by brief human vocalization. *American Psychologist*, *74*(6), 698–712. https://doi.org/10.1037/amp0000399

Dedovic, A., Rexroth, M., Wolff, E., Duchesne, A., Scherling, C., Beaudry, T., Lue, S.D., Lord, C., Engert, V., & Pruessner, J.C. (2009). Neural correlates of processing stressful information: An event-related fMRI study. *Brain Research, 1293*, 49-60. https://doi.org/10.1016/j.brainres.2009.06.044

Farrow, T. F., Johnson, N. K., Hunter, M. D., Barker, A. T., Wilkinson, I. D., & Woodruff, P. W. (2013). Neural correlates of the behavioral-autonomic interaction response to potentially threatening stimuli. *Frontiers in Human Neuroscience, 6(34), 1-17.* https://doi.org/10.3389/fnhum.2012.00349

Feast, J. (2019, November 20). 4 Ways to Address Gender Bias in AI. *Harvard Business Review*. https://hbr.org/2019/11/4-ways-to-address-gender-bias-in-ai

Fennelly, L. J. (2016). *Effective physical security* (5th ed.). Cambridge, MA: Elsevier.

Flyvbjerg, B. (2006). Five Misunderstandings About Case-Study Research. *Qualitative Inquiry*, *12*(2), 219–245. https://doi.org/10.1177/1077800405284363

Gius, D., Mieszala, J. C., Panayiotou, E., & Poppensieker, T. (October 1, 2018). Value and resilience through better risk management. Retrieved March 17, 2021, from https://www.mckinsey.com/business-functions/risk/our-insights/value-and-resilience-through-better-risk-management

Gray, D. E. (2018). *Doing research in the real world* (4th ed.). SAGE Publications.

Gustafson, C. M. (2002). Employee turnover: a study of private clubs in the USA. *International Journal of Contemporary Hospitality Management*, *14*(3), 106–113. https://doi.org/10.1108/09596110210424385

Hamel, J., Dufour, S., & Fortin, D. (1993). *Case study methods* (1st ed., Qualitative Research Methods Series 32). SAGE Publications.

Hughes, C. (2017). *The ellipsis manual: Analysis and engineering of human behavior*. Evergreen Press.

Jameson, S. M. (2000). Recruitment and training in small firms. *Journal of European Industrial Training*, *24*(1), 43-49. https://doi.org/10.1108/03090590010308255

Johnstone, T., & Scherer, K. R. (2000). Vocal Communication of Emotion. In M. Lewis & J. Haviland (Eds.), *The Handbook of Emotion* (pp. 220-235). New York: Guilford.

Junoh, A. K., Mansor, M. N., Ya'acob, A. M., Adnan, F. A., Saad, S. A., & Yazid, N. M. (2013). Crime Detection with DCT and Artificial Intelligent Approach. *Advanced Materials Research, 816-817*, 610-615. https://doi.org/10.4028/www.scientific.net/amr.816-817.610

Kaminski, P., & Schonert, J. (2017, November 07). The neglected art of risk detection. Retrieved November 14, 2020 from https://www.mckinsey.com/business-functions/risk/our-insights/the-neglected-art-of-risk-detection

Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons, 62*(1), 15-25. https://doi.org/10.1016/j.bushor.2018.08.004

Kemshall, H., Wilkinson, B., & Mackenzie, G. (n.d.). 6.1.2 False Positive and False Negatives in Risk Assessments. *In Risk of harm guidance and training resources*, Version 4.36 (Rep.). Retrieved February 18, 2021, from http://www.nomsintranet.org.uk/roh/roh/6-best_practice/06_01_02.htm

Kennedy J (2016) Shedding light on employee theft's dark figure: A typology of employee theft non-reporting rationalizations. *Organization Management Journal 13*(1): 49–60. https://doi.org/10.1080/15416518.2015.1110513

Kilichan, R., & Yilmaz, M. (2020). Artificial Intelligence and Robotic Technologies in Tourism and Hospitality Industry. *Crisis Management Skills and Strategies of Accommodation Businesses Executives, 3*, 353-380. https://www.researchgate.net/publication/348115261

Kleinberg, B., & Verschuere, B. (2021). How humans impair automated deception detection performance. *Acta Psychologica, 213*, 103250. https://doi.org/10.1016/j.actpsy.2020.103250

Knight, W. (2020, July 20). AI Is All the Rage, So Why Aren't More Businesses Using It? *Wired*. https://www.wired.com/story/ai-why-not-more-businesses-use/

Koranne, S., & Sandhu, S. (2021). Embedding Artificial Intelligence in Hospitality & Tourism. *Psychology and Education Journal, 58*(2), 5384–5389. https://doi.org/10.17762/pae.v58i2.2950

Laukka, P., Linnman, C., Ahs, F., Pissiota, A., Frans, O., Faria, V., Michelgard, A., Appel, L., Fredrikson, M., & Furmark T. (2008). In a nervous voice: Acoustic analysis and perception of anxiety in social phobics' speech. *Journal of Nonverbal Behavior, 32*(4), 195-214. https://doi.org/10.1007/s10919-008-0055-9

Mendoza, E., & Carballo, G. (1998). Acoustic analysis of induced vocal stress by means of cognitive workload tasks. *Journal of Voice, 12*(3), 263-273. https://doi.org/10.1016/s0892-1997(98)80017-9

Meyer, M., Roodt, G., & Robbins, M. (2011). Human resources risk management: Governing people risks for improved performance. *SA Journal of Human Resource Management 9*(1), Art. #366, 12 pages. https://doi.org/10.4102/sajhrm.v9i1.366

Muehlhan, M., Lueken, U., Siegert, J., Wittchen, H. U., Smolka, M. N., & Kirschbaum, C. (2013). Enhanced Sympathetic Arousal in Response to fMRI Scanning Correlates with Task Induced Activations and Deactivations. *PLOS One, 8*(8), 1-11. https://doi.org/10.1371/journal.pone.0072576
Murphy, K. R., Myors, B., & Wolach, A. H. (2014). *Statistical power analysis: A simple and general model for traditional and modern hypothesis tests*. London: Routledge.

Navarro, J., & Karlins, M. (2008). *What every BODY is saying: An ex-FBI agent's guide to speed-reading people*. New York, NY: Harper Collins.

NI Business Info. (2020). Risks and limitations of artificial intelligence in business. Retrieved December 7, 2020, from https://www.nibusinessinfo.co.uk/content/risks-and-limitations-artificial-intelligence-business

Nierenberg, G. I., Calero, H. H., & Grayson, G. (2010). *How to read a person like a book: Observing body language to know what people are thinking*. Garden City Park, NY: Square One.

Oliphant, B. J., & Oliphant, G. C. (2001). Using a behavior-based method to identify and reduce employee theft. *International Journal of Retail & Distribution Management, 29*(10), 442-451. https://doi.org/10.1108/09590550110405321

Pierce, L., & Snyder, J. A. (2015). Unethical Demand and Employee Turnover. *Journal of Business Ethics*, 1-46. https://doi.org/10.2139/ssrn.2260513

Poulston, J. (2008). Rationales for employee theft in hospitality: Excuses, excuses. *Journal of Hospitality and Tourism Management, 15*(01), 49-58. https://doi.org/10.1375/jhtm.15.1.49

Purpura, P. P. (2020). *Security and loss prevention: An introduction*. Oxford: Butterworth-Heinemann.

Quest, L., Charrie, A., de Jongh., L., & Roy, S. (2018, August 9). The Risks and Benefits of Using AI to Detect Crime. *Harvard Business Review*. https://hbr.org/2018/08/the-risks-and-benefits-of-using-ai-to-detect-crime

Rigano, C. (2019). Using Artificial Intelligence to Address Criminal Justice Needs. *National Institute of Justice Journal, 280*, 1-10. https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address-criminal-justice-needs

Robson, C., & McCartan, K. (2016). *Real world research* (4th ed.). Chichester: Wiley.

Ruiz, R., Legros, C., & Guell, A. (1990). Voice Analysis to Predict the Psychological or Physical State of a Speaker. *Aviation, Space, and Environmental Medicine*, *61*(3), 266-271. https://www.researchgate.net/publication/20839270_Voice_analysis_to_predict_the_psychological_or_physical_state_of_a_speaker

Scherer, K. (2003). Vocal communication of emotion: A review of research paradigms. *Speech Communication, 40*(1-2), 227-256. https://doi.org/10.1016/s0167-6393(02)00084-5

Simon-Thomas, E. R., Keltner, D. J., Sauter, D., Sinicropi-Yao, L., & Abramson, A. (2009). The voice conveys specific emotions: Evidence from vocal burst displays. *Emotion*, 9(6), 838–846. https://doi.org/10.1037/a0017810

Sondhi, S., Khan, M., Vijay, R., & Salhan, A. K. (2015). Vocal Indicators of Emotional Stress. *International Journal of Computer Applications, 122*(15), 38-43. https://doi.org/10.5120/21780-5056
Strickhouser, A. (2004) The Unique Challenges of Casino Security. Retrieved January 15, 2021 from https://www.ifpo.org/resource-links/articles-and-reports/protection-of-specific-environments/the-unique-challenges-of-casino-security/

Suchotzki, K., Verschuere, B., Van Bockstaele, B., Be-Shakhar, G., & Crombez, G. (2017). Meta-Analysis on Reaction Time Measures. *Psychological Bulletin, 143*(4), 428-453. https://doi.org/10.1037/bul0000087

Thorson, B. (2020, June 16). How A.I is used in the casino industry. Retrieved March 3, 2021, from https://www.tmcnet.com/topics/articles/2020/06/16/445688-how-ai-used-the-casino-industry.htm

Throckmorton, C. S., Mayew, W. J., Venkatachalam, M., & Collins, L. M. (2015). Financial fraud detection using vocal, linguistic and financial cues. *Decision Support Systems, 74*, 78-87. http://doi.org/10.1016/j.dss.2015.04.006

Tselyutina, T. V., Timokhina, O. A., Vlasova, T. A., & Maslova, Y. V. (2019). Development of the Personnel Risks Assessment and Supply Chain Strategy as a Basis of the Risk Management System of Modern Organizations. *International Journal of Supply Chain Management, 8*(5), 1030-1038. https://doi.org/10.1088/1757-899X/945/1/012021

Van Puyvelde, M., Neyt, X., McGlone, F., & Pattyn, N. (2018). Voice Stress Analysis: A New Framework for Voice and Effort in Human Performance. *Frontiers in Psychology, 9*, 1-25. https://doi.org/10.3389/fpsyg.2018.01994

Verschuere, B., Köbis, N., Meyer, Y., Rand, D. G., & Shalvi, S. (2018). Meta-analyzing the effect of imposing cognitive load. *Journal of Applied Research in Memory and Cognition, 7*, 462-469. https://doi.org/10.31219.osf.io/uqvkt

Williams, C. E., & Stevens, K. N. (1972). Emotions and Speech: Some Acoustical Correlates. *The Journal of the Acoustical Society of America, 52*(4B), 1238-1250. https://doi.org/10.1121/1.1913238

Zlatanov, S., & Popesku, J. (2019). Current Applications of Artificial Intelligence in Tourism and Hospitality. *Information Technology in Education & Digital Transformation, Culture and Creative Industries*, 84-90. https://doi.org/10.15308/Sinteza-2019-84-90