גיליון מספר 8
ספטמבר 2018

מעילות והונאות

עיונים בביקורת הפנימית

16 בינה מלאכותית והמבקר הפנימי

22 תוכנית אקטיבית לצמצום חשיפות להונאות ומעילות

48 קץ הביקורת? על הבלוקצ'יין ועתיד הביקורת

54 חמשת העקרונות לניהול סיכוני הונאות

עורכת כתב העת — **שרון ויטקובסקי טביב**, רו"ח, CIA, CRMA

סגן העורכת — **אורן שחר**, רו"ח, MBA, CISA, CIA

חברי המערכת — **דוד אגרנט**, CIA, רו"ח

שלומית איתן, עו"ד, CIA

אהוד אמינפור, CISA

דרור בר משה, רו"ח, LLM, CIA, CISA, CRMA, CRISC

יוסי גינוסר, רו"ח, CFE, CRMA, CIA

ננסי זכאכ אבו אלנסר, CPA, MA

נאוה חלמיש, רו"ח, MA

ד"ר יוסי נטוביץ, רו"ח

ליאור סגל, רו"ח, עו"ד, MBA

ד"ר גבי סייג, D.E.A

בועז ענר, רו"ח, MA, CIA

דורון רונן, רו"ח, CIA, CRMA, QAR, CRISK, CFE, MA, LLM

רונית שוורץ, MBA

מרגלית שפרבר, רו"ח, MBA, CIA

מנהלת לשכת נשיא האיגוד — **אינה גולדרביטר**

עיצוב ועריכה גרפית — **סטודיו דגה**

עריכה לשונית והגהה — **אודי לוינגר**

מו"ל — **IIA ישראל - איגוד מבקרים פנימיים בישראל בע"מ**

IIA ישראל - איגוד מבקרים פנימיים בישראל בע"מ

כתובת למשלוח דואר **ת.ד. 29281 תל אביב 61292**

טל **03-5116617** | פקס **03-5116647** | לתגובות והערות **theiiaisrael@gmail.com**

המובע במאמרים מבטא את דעת הכותבים בלבד. אין האיגוד נושא באחריות כלשהי בגין הנכתב בהם.

כל הזכויות שמורות ל- IIA ישראל - איגוד מבקרים פנימיים בישראל. ט.ל.ח

תוכן עניינים

דברים

2 דבר הנשיא

3 דבר העורכת

על המדוכה

4 משולחן האיגוד

6-7 מהנעשה בעולם

8-9 מישהו הזיז את הגבינה שלנו...

10-12 מדור מחקרים

14-15 חשד ממשי למעילה?! מה עושים?

תהליכים, טכניקות וכלים

16-21 בינה מלאכותית והמבקר הפנימי

22-25 תוכנית אקטיבית לצמצום חשיפות להונאות ומעילות

26-29 הפרצה קוראת לגנב - האם ואיך ניתן למנוע זאת?

30-33 סוף הונאה במחשבה תחילה

ממשל תאגידי

34-36 רשלנות תורמת של הארגון למעילה

38-41 הערך הכספי של ביקורות לזיהוי טעויות

42-43 הונאת השותף

44-46 מערכת ניהול למניעת שוחד (ISO 37001) ועבודת הביקורת הפנימית

מערכות מידע

48-51 קץ הביקורת? על הבלוקצ'יין ועתיד הביקורת

52-53 מניעת דלף מידע

ניהול סיכונים

54-59 חמשת העקרונות לניהול סיכוני הונאות

60-63 עמותה וקוץ בה? סיכונים מרכזיים בארגוני המגזר השלישי

64-67 סיכוני מודלים - הפעילות העסקית, המבקר הפנימי ומה שביניהם

68-70 הונאות בדיווח כספי - כיצד ניתן להתמודד עם הסיכון?

דעות ובלוגים

72-73 מיומנה של מבקרת פנימית

NOTES

74 Editor's Note

75 President's Note

דבר הנשיא

דורון כהן, רו"ח

נשיא IIA ישראל - איגוד המבקרים הפנימיים

מעת לעת מתגלית בארץ או בעולם מעילה משמעותית, ומיד נשאלת השאלה "היכן היה המבקר הפנימי?". מצד אחד, טוב שהציבור הרחב רואה בנו, המבקרים הפנימיים, גורם חשוב במניעת מעילות והונאות. מצד שני, אפשר ללמוד מכך שיש פער ציפיות לגבי תפקיד המבקר הפנימי וגבולות אחריותו. בהתאם לתקנים המקצועיים של הביקורת הפנימית, המבקר הפנימי אמור להיות בעל ידע להערכת סיכון הונאה אך לא מצופה ממנו להיות בעל התמחות בגילוי הונאות. המשמעות בפרקטיקה היא כי על המבקר הפנימי להתייחס לסיכון זה בעת קביעת תוכנית העבודה השנתית כפי שמתייחס לסיכונים אחרים ומגוונים. גם בעת ביצוע מטלת ביקורת עליו להיות ער לסיכון זה, ולהמליץ בין היתר גם על סתימת פרצות ושיפור התהליכים הקשורים. לעיתים כתוצאה מעבודת הביקורת מתגלות מעילות והונאות, ולא פעם הביקורת גם נוטלת חלק פעיל בחקירת אי סדרים שהתגלו, אך חשוב להדגיש כי זו לא המטרה והתכלית העיקריות של עבודתנו ואין לצפות כי הביקורת על משאביה המוגבלים תגלה ותמנע את כל המעילות וההונאות. אנו מאמינים כי בגיליון זה, בו החלטנו להתמקד בנושא מעילות והונאות, תכירו גישות וכלים מגוונים להתמודדות עם נושא מאתגר זה.

האיגוד נשא פרי במאמציו להשפיע על המלצות צוות בין משרדי בנושא בחינת הקמה של בורסה ייעודית לחברות קטנות ובינוניות. בדוח ביניים שיצא בנובמבר 2017, הייתה המלצה לפטור חברות בעלי היקף פעילות או מאפייני פעילות מסוימים מהחובה למנות מבקר פנימי. בהתייחסות מנומקת שפרסם האיגוד בינואר 2018, נטען כי המבקר הפנימי כשומר סף אובייקטיבי ומקצועי המשמש כשלוח של חברי הדירקטוריון, מהווה קו הגנה חשוב ביותר לארגון בלי קשר לגודלו, וכי הנחיה כאמור תפגע בציבור החוסכים ובעלי המניות, ובממשל התאגידי בחברות אלה. לשמחתנו, הדוח הסופי שפורסם ביוני 2018 לא כלל המלצה זו.

לאחרונה פרסם האיגוד התייחסות לטיוטת חוזר שפרסם יו"ר הרשות לחברות ממשלתיות בדבר פעילות הביקורת הפנימית בחברות אלה. האיגוד מברך על היוזמה לחזק את הביקורת הפנימית במגזר חשוב זה. עם זאת, לאיגוד היו השגות לגבי חלק מההמלצות, כך למשל, לדעת האיגוד חסרה התייחסות לנושא המהותי של היקף משאבי הביקורת הפנימית כך שתוכל לתפקד באופן אפקטיבי. בנוסף, האיגוד סבור כי אין לכפות על חלק ניכר מהחברות הממשלתיות התקשרות עם מבקר פנימי עובד חברה, וכי יש להשאיר את קביעת אופן ההתקשרות להחלטת הדירקטוריון.

בברכת קריאה מהנה,
דורון כהן

דבר העורכת

שרון ויטקובסקי טביב, רו"ח
CIA, CRMA

מה עבר בראשה של צעירה בת 34 שבמשך חמש שנים ניהלה חיים כפולים? מצד אחד, סגנית מנהלת מחלקת השקעות מסורה ומוערכת על ידי לקוחותיה ומנהליה, אמא לילדים ואישה נעימת הליכות. מצד שני, גונבת יותר מ-250 מיליון שקל מהבנק שבו היא עובדת, גורמת להפסקת עבודתם של חבריה לעבודה וממוטטת בנק! לזה אין לי תשובה...

אני עדיין זוכרת את הפנייה הדחופה שקיבלתי בבוקרו של יום ראשון בשבוע סטנדרטי בשנת 2002: "שרון, תגיעי דחוף לבנק למסחר עם צוות משרדי. התגלתה שם מעילה גדולה מאוד ויש צורך לכמת אותה".

היום הראשון שבו הגיעו העובדים למשרדי הבנק חרוט עד היום היטב בזיכרוני. הפליאה וההלם שהיו על פניהם של חבריה לעבודה היו בולטים. הם ישבו וסיפרו לנו על אתי חברתם, על המעשים הטובים שעשתה ועל העזרה שהושיטה לכל מי שנדרש. בשלב הזה הם עדין לא קלטו את ההשלכות של מעשיה, לקחו אותי לעמדה שלה והראו לי כמעט בגאווה את התעודה שקיבלה על היותה עובדת מצטיינת ביזמות. לקראת הצהריים חשתי ש"האסימון מתחיל ליפול" וראיתי יותר ויותר פנים נפולות שמבינות את גודל הסערה שהכתה בהם. התדהמה ממעשיה נמהלה בחשש מההשלכות עליהם ועל עתידם במקום עבודתם. בצהריים הודיעו לעובדים שהם יכולים ללכת הביתה ויעדכנו אותם לגבי ההמשך. כולנו יודעים שלא היה לזה המשך - הבנק נפל.

המסקנה האישית שלי והמסר שנחרט אצלי מאותו היום: **זה יכול לקרות בסביבה של כל אחד**! ההלם והתדהמה למשמע אירוע מעילה או הונאה חמור יכולים להיות גם מנת חלקנו, ולכן **אנחנו כמבקרים פנימיים צריכים להישאר חדים וערניים**.

אבל האם זה מספיק?

האם חדות, ערנות ואף ספקנות מקצועית יכולים בהכרח לאתר את המעילה הבאה?

בכנות, אני חושבת שלא בהכרח. הסיכוי שלא נגלה מעילה קיים, אבל אנו צריכים לעשות הכול כדי לאתרה ולא "להירדם בשמירה".

בגיליון הנוכחי בחרנו להתמקד בטכניקות ובכלים שמבקרים פנימיים יכולים לאמץ כדי להישאר ערניים ולאתר מעילות והונאות מוקדם ככל שניתן. כולי תקווה שהטמעת בקרות ושיטות חדשות, בצירוף הגברת המודעות והדריכות לנעשה בארגון ותשומת לב לפעולות חריגות, ימנעו ממועלים פוטנציאלים לבצע את המעילה הבאה או לפחות יקשו עליהם בצורה משמעותית.

ואסיים בציטוט ממסכת אבות: "**לא עליך המלאכה לגמור, ואין אתה בן חורין להיבטל ממנה**". בהקבלה לענייננו - אנו כמבקרים פנימיים לא בהכרח נאתר את כל ההונאות והמעילות בארגון, אבל מצופה מאיתנו לעשות ככל יכולתנו כדי לאתרן, ואין לנו את הזכות שלא לעשות זאת.

בברכת חג שמח וקריאה מהנה,
שרון ויטקובסקי טביב

התייחסות IIA ישראל - איגוד מבקרים פנימיים בישראל

המלצות הצוות הבין משרדי לבחינת הקמתה של בורסה ייעודית לחברות קטנות ובינוניות

בגיליון הקודם הבאנו לידיעתכם כי האיגוד פרסם בנייר עמדה מפורט את השגותיו להמלצות דוח הביניים שפורסם בנובמבר 2017, וכלל בין היתר פטור מחובת מינוי מבקר פנימי במקרים מסוימים.

אנו שמחים לדווח כי בעקבות ההתייחסות המקיפה ששלח האיגוד, הוסרה המלצה בעייתית זו מהדוח הסופי שפורסם ביוני 2018.

טענות האיגוד היו כי פטור כזה יגרום לפגיעה משמעותית בחברות עצמן ובמשטר התאגידי שלהן, יפגע בציבור החוסכים ובבעלי המניות, וזאת לאור חשיבותו של המבקר הפנימי כשומר סף מקצועי ובלתי תלוי, שלוח של הדירקטוריון, הבוחן בין היתר עסקאות עם בעלי עניין ומסייע במניעת גילוי הונאות ואי סדרים.

משולחן האיגוד

התייחסות IIA ישראל - איגוד מבקרים פנימיים בישראל

טיוטת חוזר רשות החברות בדבר כללים להבטחת יעילות ותקינות הביקורת הפנימית בחברות ממשלתיות

לאחרונה פרסמה רשות החברות טיוטת חוזר בנושא הנ"ל. האיגוד שלח לרשות את התייחסותו המפורטת לטיוטה ואף פרסם את התייחסותו ברשתות החברתיות ובאתר האיגוד. בהתייחסותו מברך האיגוד על היוזמה לחיזוק הביקורת הפנימית במגזר חשוב זה. עם זאת, לאיגוד היו מספר השגות מהותיות להמלצות המופיעות בטיוטה ובהן:

חוסר התייחסות להבטחת אפקטיביות הביקורת הפנימית באמצעות הקצאת משאבים הולמים, הבהרת היבטי כפיפות המבקר הפנימי (שנכון להיום היא דואלית בהתאם לחוק החברות הממשלתיות). בנוסף, האיגוד סבור כי החוזר מפלה בין מבקרים פנימיים עובדי החברות הממשלתיות למבקרים פנימיים נותני שירותים, ומערער על סמכות ואחריות הדירקטוריון בנושא זה. האיגוד צירף לחוות דעתו המקצועית חוות דעת משפטית לגבי הנושא האמור לעיל ולגבי תהליך פרסום ואישור החוזר בכללותו.

קישור לחוות דעת האיגוד ניתן למצוא באתר האיגוד.

מעילות והונאות לפי תקני ה-IIA

גיליון כתב העת מוקדש הפעם לנושא מעילות והונאות. בתקנים של ה-IIA יש כמה התייחסויות לתפקידי המבקר הפנימי בנושא הונאות ומעילות, ואלה העיקריות שבהן:

1. הגדרת מילון המונחים IPPF להונאה: כל מעשה בלתי חוקי שמאופיין על ידי תרמית, הסתרה, או הפרת אמונים. מעשים אלה אינם תלויים ביישום איומים או אלימות או כוח פיזי. הונאות מבוצעות על ידי צדדים וארגונים כדי להשיג כסף, רכוש או שירותים; להימנע מתשלום או הפסד שירותים; או כדי להבטיח יתרון עסקי או אישי.
2. תקן 1210.A2:"מבקרים פנימיים חייבים להיות בעלי ידע מספק כדי להעריך **סיכון להונאה**, ואת האופן שבו הוא מנוהל על ידי הארגון. עם זאת, אין לצפות מהם להיות בעלי ההתמחויות של מי, שתפקידו העיקרי הוא לגלות ולחקור הונאות".
3. תקן 1220.A1:"מבקרים פנימיים חייבים לנהוג בזהירות מקצועית ראויה על ידי הפעלת שיקול דעת בנושאים הבאים:
   - היקף העבודה הדרושה להשגת יעדי מטלות הביקורת;
   - מורכבות יחסית, מהותיות ומשמעותיות של עניינים, שלהם מיושמים נוהלי שירותי ההבטחה;
   - נאותות ואפקטיביות של תהליכי ממשל תאגידי, ניהול הסיכונים, ותהליכי הבקרה;
   - **הסתברות** לטעויות משמעותיות, **לאי-סדרים (הונאות)**, ולאי-ציות;
   - עלות שירותי ההבטחה יחסית לתועלת הפוטנציאלית מהם.
4. תקן 2060 (דיווח להנהלה הבכירה ולדירקטוריון): "**המבקר הפנימי הראשי חייב לדווח באופן תקופתי להנהלה הבכירה ולדירקטוריון אודות** המטרות, הסמכות, האחריות והביצועים של הביקורת הפנימית בהשוואה לתוכנית העבודה ועל עמידתה בקוד האתי ובתקנים. הדיווח גם חייב לכלול נושאי סיכונים ובקרות משמעותיים, לרבות **סיכוני הונאה**, נושאי ממשל תאגידי, ונושאים אחרים הדורשים את תשומת הלב של ההנהלה הבכירה ו/או הדירקטוריון.
5. תקן 2120.A2: "הביקורת הפנימית חייבת להעריך את **הפוטנציאל להתרחשות הונאה וכיצד הארגון מנהל סיכוני הונאה**".
6. תקן 2210.A2: "במהלך קביעת מטרות מטלת הביקורת, מבקרים פנימיים **חייבים לשקול את ההסתברות של** טעויות משמעותיות, **הונאות**, אי-ציות וחשיפות אחרות".

יום חמישי, 17.1.2019 • Avenue, Airport City

אנשים ומחשבים

לרישום מח' אירועים טל' 03-7330777 או באתר iia-event-2019.events.co.il
לחסויות: נטלי 03-7330770 natali@pc.co.il

מהנעשה בעולם

קלות השוחד

עשרות מיליוני אנשים משלמים שוחד ברחבי חצי הכדור המערבי.

כמעט 30% מתושבי אמריקה הלטינית והאיים הקריביים שילמו שוחד עבור השימוש בשירותים ציבוריים חשובים, כגון בתי ספר, שירותים עירוניים ובתי משפט במהלך 12 החודשים האחרונים, כך מדווח ארגון Transparency International (TI) שנחשב ל"כלב שמירה" חובק עולם נגד השחיתות.

הדוח, שכותרתו הוא "אנשים ושחיתות: אמריקה הלטינית והאיים הקרביים", מקביל את האחוזים הללו ל-90 מיליון אנשים המתגוררים ב-20 הארצות שנדגמו.

למרות מחאות המוניות נגד שחיתות שנערכו לאחרונה באזור, כמעט שני שלישים מ-22,000 התושבים שנדגמו סבורים שחלה עלייה ניכרת במקרי השחיתות בארצם. רק 10% מהם סבורים שהשחיתות הצטמצמה. היו"ר של TI, חוזה יוגז, סבור כי "שוחד מהווה אמצעי להתעשרות מעטים, והוא אף מהווה מחסום משמעותי להנגשת שירותים ציבוריים חיוניים, במיוחד לאנשים החלשים ביותר בחברה".

כמעט מחצית מהמשיבים טוענים שמרבית הפוליטיקאים והשוטרים במדינתם מושחתים - וזאת באחוזים גדולים יותר מכל מוסד אחר. 53% סבורים שממשלתם אינה מטפלת בביעור השחיתות באופן יעיל, ו-35% טוענים שהנושא מטופל בצורה נאותה.

כדי להיאבק בשחיתות באזור, ממליצה TI לחזק את שלטון החוק, להציע לתושבים אמצעים סודיים כדי לדווח על חוויותיהם עם השירותים הציבוריים, וכן לחזק את המוסדות שמטפלים בפשעים הקשורים בעבירות שחיתות.

D. Salierno

לבינה מלאכותית יש השפעה אמיתית:

צוותי אבטחה טוענים שבינה מלאכותית מעניקה להם יתרון על פני תוכנות כופר ופרצות מידע

81% אומרים שבינה מלאכותית מגלה איומים זדוניים עוד לפני צוותי האבטחה שלהם

78% אומרים שבינה מלאכותית מגלה איומים שבני אדם אינם מסוגלים לראות

77% אומרים שהשימוש בכלים המופעלים על ידי בינה מלאכותית מונע פרצות נוספות

70% אומרים שצוותי האבטחה עושים שימוש בבינה מלאכותית באסטרטגיות מניעת איומים של הארגון

מקור: Cylance, Artificial Intelligence in the Enterprise

חיזוק הבקרה והפיקוח

שערוריות גורמות לתעשייני יפן להגביר את הבקרות הפנימיות.

בעקבות השערוריות האחרונות בקרב התעשיינים המובילים ביפן, נערך סקר על ידי חברת Nikkeei Research בקרב כ-500 חברות יפניות גדולות ובינוניות. כ-90% מהחברות שנסקרו חוששות שלשערוריות הללו תהיה השפעה שלילית על המוניטין של יפן ליצור מצוינות, ולמעלה מרבע מאותן חברות מביעות דאגה רבה מכך.

בשנה שעברה הודו מספר ספקים יפנים גדולים שסילפו נתוני מידע. חברת סובארו הודיעה בדוח שנשלח לממשלת יפן שתחזק את הציות לאחר שהודתה שטכנאים לא מוסמכים ביצעו מבדקים שאינם בסמכותם לרכבים במהלך 30 השנים האחרונות. החברה הסבירה שההנהלה והעובדים לא העריכו מספיק את חשיבותם של המבדקים.

כמו במקרה של סובארו, בסקר עולה שכמעט מחצית מהחברות (כ-44%) טוענות שהן פועלות להגברת בקרת האיכות כתגובה לשערוריות. הצעדים שהן נוקטות כוללים: שיפור והעמקת ההדרכות בנושאי ציות ופיקוח על מוצרים, בחינת התקנות, וביצוע מבדקי פתע.

T. MCCOLLUM

95% ממומחי אבטחת מידע
טוענים שלמידת מכונה מהווה מרכיב חיוני של אסטרטגיית אבטחת סייבר

87% מדווחים שהארגונים שלהם עושים שימוש בבינה מלאכותית
במערך אבטחת הסייבר

75% אומרים שבמהלך שלוש השנים הבאות
תתקשה החברה שלהם להגן על נכסים דיגיטליים ללא בינה מלאכותית

"אין ספק שבינה מלאכותית מהווה את עתיד האבטחה, נוכח העובדה שבני אדם מתקשים מאוד לעקוב לבדם אחר היקף האיומים"

כך אומר הל לואנס, מנהל טכנולוגיה ראשי בחברת Webroot Cybersecurity & Threat Intelligenc Services

מקור: Webroot and Wakefield Research, Game Changers
בינה מלאכותית ולמידת מכונה באבטחת סייבר

מישהו הזיז את הגבינה שלנו...

והפעם במדור: על איתור מוקדם של מעילות באמצעות אינדיקטורים התנהגותיים ועל שיתוף פעולה בין סטארט-אפ ליחידת ביקורת

מאת
מרגלית שפרבר | רו"ח, MBA, CIA
מבקרת פנימית ראשית, תנובה

בשנים האחרונות מתגברת הפגיעה במשאבים ובאינטרסים של החברה על ידי עובדיה. ממחקרים עולה כי למעלה מ-69% ממקרי הפגיעה המשמעותית בארגונים בעולם בוצעו במעורבות של עובדי הארגון.

אנחנו כמבקרים נדרשים להתמודד עם השאלה: עד כמה אנחנו מצליחים לאתר את הפגיעות ובאיזה שלב?

על מנת להעלות את הסיכויים לאיתור מוקדם של התנהגויות חריגות, נכנסנו ביחידת הביקורת של תנובה לפיילוט טכנולוגי עם פרדיקטיקו, חברת סטארט-אפ ישראלית שפיתחה שיטה לאיתור מוקדם של התנהגויות חריגות באמצעות ניתוח נתוני ביג-דאטה, בהתבסס על אינדיקטורים התנהגותיים.

שיתוף פעולה בין סטארט-אפ ליחידת ביקורת איננו שכיח במחוזותינו והוא מאתגר את שני הצדדים. במסגרת פינת החדשנות בגיליון זה, רציתי לשתף בחוויה המרתקת והמורכבת שלנו בתנובה עם פרדיקטיקו.

רקע: פיילוט ראשון נערך בחברה גלובלית

2015 - פיילוט ראשון נערך בחברת ענק גלובלית המעסיקה כ-20 אלף עובדים ברחבי העולם, מתוך כוונה לתת מענה לאתגרי פגיעה של עובדים. החברה טיפלה לאורך שנים במקרים רבים וכואבים של פגיעות פנימיות - מקרי גניבה, הונאה, פגיעה במוניטין ואף העברת מידע תחרותי למתחריה. ניסיונותיה של החברה לאתר אירועים אלה באמצעים הטכנולוגים המקובלים (מערכות ניטור, מערכת שערי הכניסה) לא צלחו, וחרף המאמצים כמות האירועים לא ירדה. להיפך, עם השנים הסיכונים התרבו וגילויים התרחשו מאוחר מדי - לעיתים באופן מקרי ורק לאחר עזיבתו של העובד.

צוות פרדיקטיקו, המורכב משותפים מדיסציפלינות מקצועיות מגוונות, שם לו למטרה לאתר התנהגויות חריגות על סמך נתונים תפעוליים קיימים המשמשים לצרכים ניהוליים שוטפים. זאת מתוך מוטיבציה לצמצום הצורך באמצעים חודרניים כגון מצלמות, מערכות ניטור, בדיקות פוליגרף או מידע מהרשתות החברתיות, ומתוך שמירה מקסימלית על חיסיון פרטי המידע הרגישים של העובדים.

2016 - פריצת דרך בגיבוש שיטת העבודה החדשה הושגה כאשר לצוות הצטרף פרופ' יואב ורדי, והביא עימו מודלים התנהגותיים שנאספו לאורך השנים. אלו אפשרו למקד את המידע הארגוני הנדרש ולהטמיע בתוכנה את כל התובנות של כ-80 אינדיקטורים התנהגותיים בודדים על תצריפיהם.

הפיילוט הראשון שלהם בחברת הענק הגלובלית הסתיים בהצלחה ב-2016. בסיומו אותרו סיכונים ברורים בקרב עובדים בודדים וקבוצות עובדים שונות בחברה. מרבית הסיכונים הללו לא היו ידועים בשעתו להנהלת החברה וטופלו מיידית על מנת למנוע את התפתחותם.

תוצאות אלו שכנעו את הנהלת החברה הגלובלית לאמץ את השיטה ולהאיץ בצוות הסטארט-אפ לפתח את הרכיבים הטכנולוגיים הנדרשים כדי להטמיע את הכלי בסביבה הארגונית. בתום מספר חודשי פיתוח עמדו לרשות הצוות מגוון יכולות לעיבוד בסביבת ביג-דאטה, שכבת אלגוריתמים לומדים, תוכנת הצגה בסיסית של הסיכונים, ומודול ניהול שמאפשר למנהל המערכת לבצע כיול מהיר של האינדיקטורים ולהוסיף תרחישי סיכון ספציפיים לארגון.

שיתוף פעולה עם יחידת ביקורת תנובה להטמעת אב-טיפוס

2017 - בשלב זה, לאחר שהיה בידי פרדיקטיקו אב-טיפוס, נערכה פגישה ראשונה בין חבריה לצוות הביקורת הפנימית של תנובה וסיכמנו להתקדם לפיילוט טכנולוגי. כולנו זיהינו את הפוטנציאל ואת ההזדמנות לתקף את הכלי, ולהשפיע על מאפייניו באופן שיאפשר איתור מוקדם של אירועים התנהגותיים חריגים לפני התפתחותם של אי סדרים בהיקפים כואבים.

אחד האתגרים המשותפים בהטמעת האב-טיפוס בתנובה היה הקושי לאסוף במהירות וביעילות את המידע.

אתגר נוסף היה התגברות על ההבדלים בין שני הפיילוטים וביצוע התאמות מהירות ומדויקות. בין היתר: התאמות בתרחישי סיכון, והצורך בהוספת אינדיקטורים ייחודיים לתנובה על מנת להשיג הטמעה מדויקת של כלל השינויים בתוכנה שהולכת ומתפתחת בהתמדה.

ו.... התוצאות:

כמו בפיילוט הראשון, גם בתנובה התקבלו בסיומו של הפיילוט חיווי סיכון שהוכיחו שהמערכת "מפתחת חוש ריח" בזמן קצר ביותר.

בשל חיסיון המידע לצערנו לא נוכל לספר ולהדגים באשר לתוצאות. נוכל לספר על הלמידה וההתפתחות בסטארט-אפ וביחידת הביקורת.

העבודה ההדוקה ושיתוף הפעולה בין הצוותים תרמה להבשלת המוצר, כמו גם ליצירת מפת דרכים עתידית להמשך פיתוחו. תוך כדי העבודה המשותפת נחשפו אנשי הסטארט-אפ לאופי הפעילות ולזרימת המידע השוטפת ביחס לחריגים שונים והיכולת לנתחם במחלקת הביקורת. התברר שזהו מידע רב ערך מבחינת הבנת התוצאות שמספקת המערכת.

כמו כן, העבודה בשיתוף פעולה עם הביקורת אפשרה להרחיב את סל השימושים של המוצר הסופי כמוצר שמתאים גם לשימוש ביחידות ביקורת.

מצד שני, אנחנו בביקורת נחשפנו לדרך עבודתו של סטארט-אפ טכנולוגי המנסה לייצר מכונה שעובדת 24X7, ו"מבינה" רק אם יש לה הרבה דאטה ומינימום מגע יד אדם.

> כחלופה לשימוש באמצעים הטכנולוגיים המקובלים שיעילותם פוחתת, יש לשאוף לאתר אי סדרים מתוך מידע תפעולי קיים המבוסס על אינדיקטורים התנהגותיים.

מלבד יכולות האיתור המוקדם של הסיכונים, נראה כי יש למערכת תועלות נוספות עבור יחידת הביקורת, בין היתר:

1. לצורך בדיקה מהירה של פניות למוקד פניות עובדים.
2. לבחירת מדגמים חכמים כחלק ממשימת הביקורת הגמישה.
3. בסיוע למיקוד ותעדוף נושאי ביקורת על פי חיווי המערכת.
4. ליצירת שיתוף עם פונקציות סיכון ובקרה רלוונטיות בארגון.

מה צופן לנו העתיד?

לצד ההתקדמות הרבה, עוד עבודה רבה לפנינו... עד העלייה לאוויר של המערכת המלאה נדרשות השלמות מודולים של האנליטיקה, וכן תחקור ולמידת מכונה שיסייעו בהצפת תובנות מפתיעות שלא נחקרו עד כה ואף כאלה שאינן מתיישבות עם השכל הישר ואינן ניתנות לתכנון מראש.

אנו מקווים כי בעתיד סט היכולות הטכנולוגיות הגלומות בתוכנה המוטמעת בארגון ולומדת אותו באופו רציף, יאפשר לצוות הביקורת להקדים תרופה למכה ולסייע בתהליך הביקורת במגוון רחב של היבטים.

מדור מחקרים

מאת

ד"ר גבי סייג |
מרצה וחוקר בית הספר למדעי המדינה -אוניברסיטת חיפה
מנהל אקדמי של תוכנית מבקרים פנימיים - היחידה ללימודי המשך, אוניברסיטת חיפה

- הונאה (Fraud) ניתנת להגדרה כפעולה או מהלך של רמאות הנעשים ביודעין ובמגמה להונות, לכזב, או לפגוע בזכויותיו החוקיות של אחר, כדי לזכות ברווח שלא כחוק או ביתרון בלתי הוגן. הונאה כוללת מצג שווא ביודעין, או העלמה ביודעין, של עובדה מהותית, במטרה להשפיע על אחר לפעול או להימנע מלפעול בצורה מסוימת.
- במקרים לא מעטים, אי גילוי ההונאות קשור לכשל של רואי החשבון המבקרים מלזהות את הטעויות והזיופים שבוצעו בדוחות הכספיים.
- ארגונים רבים נפלו קורבן למעילות והונאות ובדרך כלל הנזקים גבוהים מאוד. על מנת להגן על המידע הפיננסי ועל מידע אחר, נדרשת מערכת בקרה אפקטיבית שתזהה ותמנע חריגות, וכאן יכולה לבוא לידי ביטוי עבודתו של המבקר הפנימי.

מהמחקר האקדמי עולה שפעילות שמטרתה מניעת הונאות בתאגידים היא חלק בלתי נפרד מעבודת הביקורת הפנימית.

- חשוב מאוד שלמבקר הפנימי יהיה תפקיד פעיל על מנת למנוע פעילות זו. כל ארגון וחברה צריכים ליצור סביבה חיובית של ביקורת פנימית, לייסד מערכת בקרה פנימית אפקטיבית, לגייס מבקרים פנימיים מקצועיים ובעלי ניסיון, ולהכשיר אותם על מנת למנוע אפשרויות למעילה תוך פיתוח אסטרטגיה של מניעה.

במדור אני מציג ארבעה מחקרים רלוונטיים:

1. הקשר בין אפקטיביות הביקורת הפנימית לחשיפת הונאות

George, D. & al. 2017. **The effect of Internal audit effectiveness, auditor responsibility and training in fraud detection .Accounting and Management Information Systems** 16(4): 434-454

המחקר הינו מחקר אמפירי שבודק את הקשר בין אפקטיביות הביקורת הפנימית (IA effectiveness - IAE), האחריות (IA Responsibility - IAR) וההכשרה (IA Training- IAT) של המבקר הפנימי לבין גילוי הונאות. (Fraud Detection - FD) תוצאות המחקר מצביעות על קשר מובהק בין IAE, IAR ו-IAT לבין FD. **למעשה, המחקר הזה נותן תוקף מדעי למאפיינים של הביקורת הפנימית המשפיעים על חשיפת הונאות.**

כדי לחקור את הקשר בין המשתנה התלוי FD (גילוי הונאות) למשתנים בלתי תלויים (IAE אפקטיביות הביקורת הפנימית), IAR (אחריות הביקורת הפנימית), ו-IAT (הכשרת הביקורת הפנימית), הסקר נערך באמצעות שאלונים שנשלחו ל-207 חברות ציבוריות הנסחרות בבורסה לניירות ערך באתונה. שיעור ההחזר הגיע ל-54% ולכן המחקר התבסס על 112 חברות מסקטורים שונים שהסכימו לענות.

השאלון כלל חמישה חלקים: החלק הראשון הציג נתונים דמוגרפים של המשיבים, וארבעת החלקים הבאים התייחסו לאיסוף נתונים אודות המשתנים של מודל המחקר באמצעות סקלת Likert באורך 5. המחקר עשה שימוש בניתוח גורמים כדי לבדוק את התוקף ואת המהימנות של השאלונים וכמובן של המשתנים. פונקציית הרגרסיה של המחקר הייתה:

$$FD_i = \beta_0 + \beta_1 IAE_i + \beta_2 IAR_i + \beta_3 IAT_i + \varepsilon$$

תופעת המעילות וההונאות והממשק לביקורת הפנימית ככלי מניעה וחשיפה

ותוצאות הרגרסיה מובאות להלן.

Depedent Variable	DF	
	Standardized Coefficients	Signifance
IAE	0.292	0,001
IAR	0.274	0,001
IAT	0.261	0,003
R Square	0.367	
F Statistics	20.850	
Durbin - Watson	1.997	

תוצאות הרגרסיה הנ"ל מראות שברמת ביטחון של 99% קיים קשר סטטיסטי מובהק בין אפקטיביות הביקורת הפנימית ואחריותו והכשרתו של המבקר הפנימי, לבין גילוי הונאות.

כלומר ניתוח תוצאות הרגרסיה מראה כי:

קיים קשר חיובי בין אפקטיביות הביקורת הפנימית, אחריותו והכשרתו של המבקר הפנימי, לבין חשיפת הונאות.

תוצאות מחקר זה מבליטות את חשיבותה של הביקורת הפנימית בגילוי הונאות, ואת הצורך הקיים בחברות להשקיע בתהליכי הביקורת הפנימית ובהכשרה על מנת להשיג ממשל תאגידי יעיל. כמו כן, המחקר מדגיש את חשיבותה של הביקורת הפנימית בגילוי מעילות בחברות הפועלות במדינות הנמצאות במשבר כלכלי.

2. הביקורת הפנימית כקו הגנה מהותי במאבק בהונאות

William,H., Carl,P., & David, S. 1999. **The internal auditor as fraud-buster. Managerial Auditing Journal** 14(7): 351-363

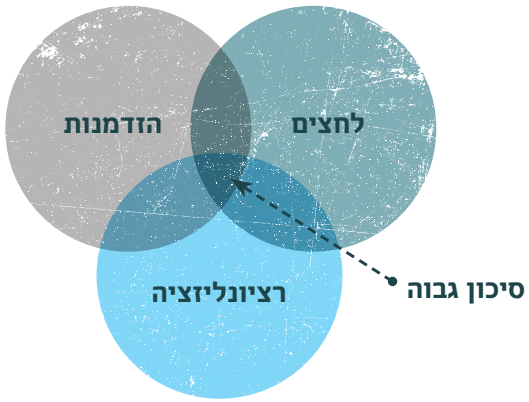
המחקר מציג את מודל ההונאות ואת שלושת עמודי התווך שלו, תוך דגש על הסיכון ההולך וגדל להונאות בארגון. החוקרים מגיעים למסקנה ש:

הביקורת הפנימית מהווה קו הגנה עיקרי נגד הונאות ומעילות שמבצעים עובדים ויש לחזקה.

בדרך כלל רואי החשבון - המבקרים החיצוניים - אינם בעמדה המאפשרת להם לגלות ולדווח על התרחשות של הונאות שמקורן בעובדי הארגון. למרות זאת, **המבקרים הפנימיים יכולים להוות את קו ההגנה הראשי כנגד הונאות בתוך הארגון.** בעבודה זו החוקרים מזהים את הנקודות הבאות: סיכוני הונאות וסימנים נוספים שבכוחו של המבקר הפנימי לאתר; הסיוע שמבקרים פנימיים יכולים להעניק למבקרים החיצוניים רואי החשבון בהטמעת תקן SAS No 82 המתאר את האחריות של המבקר רואה החשבון לגבי הונאה בדוחות הכספיים ומספק קווי פעולה כדי לשאת באותה אחריות; ציות לדרישות השונות של הרגולציה; והשלבים החיוביים שבכוחם של המבקרים הפנימיים ליישם כדי להתריע, לחשוף ולדווח על הונאות.

עם זאת, העתיד לא נראה מבטיח, מכיוון ששלושת ההיבטים של מודל ההונאות (לחצים, הזדמנות ורציונליזציה - ראה להלן) נעים בכיוון של הגדלת הסיכון למעילות. הלחצים נובעים מהאילוצים הכלכליים המיידים הרובצים על תחושות של עובד זה או אחר בארגון. ההזדמנות להונאה יכולה לנבוע ממצב שבו עובד משיג דרגה גבוהה של אמינות בארגון, או לחילופין כשהבקרה הפנימית חלשה או כמעט לא קיימת. הרציונליזציה מתייחסת למצב שבו העובד שמבצע את ההונאה יכול להצדיק את התנהגותו במסגרת תפיסתו האישית של הקוד האתי והתנהגות ראויה. לאור הגידול ב"ביקוש" להונאות, **המסקנה המתבקשת היא שיש לחזק את הביקורת הפנימית המהווה קו הגנה עיקרי.**

מודל ההונאות (Fraud Model)



3. אפקטיביות פונקציית הביקורת הפנימית בחשיפת הונאות

Paul, C., Colin, F., & Robyn, M. 2008. Internal audit, alternative internal audit structures and the level of misappropriation of assets fraud. **Accounting and Finance** 48(4): 543-559

ביקורת פנימית היא חלק חיוני במערכת של ממשל תאגידי. כיום, ישנה דאגה ציבורית משמעותית לגבי גודל ההונאות המתבצעות בתוך הארגונים. המטרה של עבודה זו הייתה להעריך באיזו מידה יש דיווח של הונאות בארגונים בהם קיימת פונקצייה של ביקורת פנימית לעומת ארגונים בהם משתמשים בשירותי ביקורת פנימית / מיקור חוץ (Outsourcing). נתונים על הונאות בתחום הנכסים נלקחו מהסקר של KPMG שבוצע בשנת 2004. הסקר התייחס ל 491 חברות בסקטור הציבורי והפרטי במדינות אוסטרליה וניו זילנד שדיווחו על הונאות. נתונים על מבנה הביקורת הפנימית באותן חברות נגזרו מתוך סקר נפרד שבוצע בקרב אותן חברות. ממצאי העבודה מצביעים בסבירות גבוהה יותר שמידת הדיווח של הונאות גבוהה יותר באותן חברות בהן קיימת פונקצייה של ביקורת פנימית. זאת, לעומת החברות המשתמשות בשירותי ביקורת פנימית חיצוניים. יוצא אפוא, שהמשך קיום של ביקורת פנימית בתוך הארגון הוא אפקטיבי יותר בדיווח הונאות לעומת המצב בו כל שירותי הביקורת הפנימית ניתנים באמצעות מיקור חוץ. מסקנה נוספת של המחקר היא ששימוש במיקור חוץ וגם בגורם פנים לביצוע עבודת הביקורת הפנימית עדיף לצורכי דיווח על הונאות ומעילות.

יחד עם זאת יש לציין שמחקרים קודמים, (Low et al.1999) (James 2003) לא מצאו הבדלים בדיווח על הונאות ומעילות אם מדובר בשכירת שירותי ביקורת פנימית או בהעסקה של מבקר פנימי בארגונים השונים. יתרה מכך מחקרם של (Carey et al.2006) מצביע על מיקור חוץ של הביקורת הפנימית כמתאים יותר לדיווח אי-סדרים ומעילות.

Carey, P., G. Tanewski, and R. Simnett, 2000, Voluntary demand for internal and external, auditing by family businesses, **Auditing: A Journal of Practice and Theory** 19, 37–51

James, K. L., 2003, The effects of internal audit structure on perceived financial statement, fraud prevention, **Accounting Horizons** 17, 315–327.

4. תפקידו של המבקר הפנימי בחיזוק הבקרה ובצמצום הונאות

Ruse E., Susmanshi, G., & Spineanu,G.L 2013. **Internal Audit and Fraud Detection."Ovidius" University Annals, Economic Sciences Series**,13(1): 1475-1479

המחקר תיאורטי בעיקרו, ומתמקד בהצעות ובהמלצות של המבקר הפנימי לנתינת מענה לסיכונים הקיימים להתרחשותן של הונאות. זאת לאחר דיון מעמיק במהותה ותפקידיה של הביקורת הפנימית, במושג של הונאות (Fraud), בקשר בין הביקורת הפנימית לבין הונאות, ובתפקידה של ההנהלה.

מהמחקר עולה שניהול חברות דורש בקרה תמידית ושיטתית וכפועל יוצא ניתן לנהל ולפתח ישויות כלכליות, ציבוריות או פרטיות ללא מערכת בקרה קפדנית, עדכנית וגמישה. **חלק מתפקידיו של המבקר הפנימי בישות הכלכלית הוא להביא להנהלה הצעות והמלצות כדי לחזק את הבקרה ולצמצם את האפשרות להונאות.** מבחינה זו, מבקרים פנימיים חייבים להביא בפני ההנהלה כל מידע שיכול להצביע על חשד לקיומה של הונאה ולסייע להנהלה בפעולתה.

איגוד מבקרים פנימיים בישראל
INSTITUTE OF INTERNAL AUDITORS IN ISRAEL

אתר האיגוד לשירותכם

תוכלו למצוא באתר

- תקינה ומידע מקצועי ממוין לנושאים לפי קטגוריות
- חדשות ועדכונים על חידושים במקצוע
- בלוגים ודעות בנושאים שונים
- כתבי עת קודמים לקריאה דיגיטלית
- קורסים וערבי עיון
- כנסים בארץ ובחו"ל

WWW.THEIIA.ORG.IL

ON AIR

הידעת? מחקרים מוכיחים שאנשים זוכרים רק:

כ-10% ממה שהם שומעים

כ-20% ממה שהם קוראים

וכ-80% ממה שהם רואים

גם דוח הביקורת שלכם יכול להיות מעוצב

סטודיו דגה - אינפוגרפיקה ועיצוב מידע

Daga GRAPHIC DESIGN STUDIO

www.daga.co.il | office@daga.co.il | 077-5044740/1

חשד ממשי למעילה?! מה עושים?

חשד ממשי למעילה או הונאה? זהירות! אין לפעול אינסטינקטיבית!

מאת

אשר ויצמן | משרד ויצמן יער חקירות

לאחרונה, וכפי שהדבר משתקף בפעילות משרדנו, קיימת עלייה בהיקף תופעת המעילות וההונאות בחברות מסחריות ובעסקים בינוניים וגדולים.

מרגע שגילתה הביקורת או ההנהלה את החשד למעילה או להונאה, הדחף האינסטינקטיבי הוא קודם כל לעמת את החשוד מול החשד ולקבל את תגובתו, או לחילופין לגשת מיד ולהתלונן במשטרת ישראל. בפועל הניסיון מלמד כי שתי הפעולות יפגעו בסופו של יום בתהליך חשיפת המעילה. במאמר זה נפרט מהו הטיפול הנכון המומלץ במצב זה.

יש למתן את הדחף האינסטינקטיבי בעימות המועל מול החשד ודרישה לקבלת תגובתו

עימות המועל מול החשד?

המגלה עשוי לסבור, ואולי בצדק, שקבלת תגובה מהחשוד תקדם מבחינתו את חשיפת הפרשה, אולם ניסיוננו מלמד כי פעולה זו שגויה ועשויה להסב נזק בלתי הפיך לסיכוי לקבל מהמועל הודאה ו/או להגיע להיקף האמיתי של המעילה או ההונאה, וכן להשבת הכספים שנגנבו.

חקירה של חשוד צריכה להיעשות אך ורק בידי חוקר מקצועי, כשבאמתחתו מידע רלוונטי על האירוע.

חשוד שנחקר עשוי להגיב להאשמות שיוטחו בו באחת משתי דרכים:

האחת - הודאה חלקית במעשים מינוריים, תוך שהוא מנסה להסתיר את ההיקף האמיתי של האירוע.

השנייה - הסתגרות טוטאלית מיד בתחילת התשאול או החקירה ואי שיתוף פעולה לחלוטין עם הגורם החוקר.

כדי לקבל הודאה מהנחקר, לחוקר המקצועי חייב להיות מידע אמיתי ומדויק שבו יעשה שימוש בנקודת זמן ספציפית וקריטית.

ברוב המקרים הנחקר עצמו לא יודע כמה מידע יש באמת בידי החוקר, ובשלב זה מנהל החוקר סוג של משחק פוקר מול הנחקר תוך יצירת מצג שלפיו הוא יודע הכול על האירוע ותוצאותיו.

מדובר בטכניקת חקירה המחייבת מיומנות מקצועית גבוהה תוך הסתייעות בעזרים שונים במהלך החקירה, כאשר החוקר יודע "לקרוא" את הנחקר ואת שפת הגוף שלו, ומנהל את החקירה בהתאם.

שימוש מושכל ומדויק של החוקר בנתונים נכונים על נקודות רלוונטיות או קריטיות באירוע, יאפשר במרבית המקרים קבלת הודאה פרטנית מהחשוד תוך עיגון הממצאים בעדות או בהקלטה סמויה.

טכניקות חקירה כאלה יושמו על ידינו למשל בחשיפת המעילה בחברת התקשורת פרטנר, שם מצאנו שהמועל ניהל חשבונות כפולים מול ספק שבתמורה קנה בכספי השוחד נכס (משרד) לחשוד המועל.

ההודאה שגבינו מהחשוד גרמה להרשעתו בתיק הפלילי ולהכרעה חד-משמעית בתיק האזרחי (תביעת נזיקין שהוגשה בידי החברה נגד המועל לאחר מכן).

גם בפרשיית המעילה בחברת נגב, שם העלתה חקירתנו מעילות בהיקף של מיליוני שקלים מצד המנכ"ל ועובדים נוספים, נאסף טרם חקירת החשודים מידע וחומר רב. חשיפתו בזמן ובעיתוי הנכונים תוך שימוש בטכניקות האלה מול כל נחקר, גרמה לכך שהצלחנו לגבות הודאות מפורטות מכל נחקר ולקבל מידע וראיות על היקף המעילה והשותפים לה.

תלונה במשטרה? מתי?

תלונה למשטרה עשויה לכאורה למצות עם החשוד את הדין. כאן עולה שאלת עיתוי התלונה למשטרה.

מתברר כי במרבית המקרים משטרת ישראל בתחנות השונות אינה ערוכה או שאין ברשותה כוח אדם מתאים לחקירות הונאה/מעילה (למעט יחידות איכותיות כמו להב 433 או יחב"ל).

המשמעות היא שברוב המקרים החקירה המשטרתית לא תנוהל בדחיפות המתבקשת, ובדרך כלל גם לא בידי כוח אדם מקצועי שיתקשה להיכנס לעובי הקורה ולהיבטים המקצועיים של העסק הספציפי שבו אירעה המעילה.

המשטרה איננה ערוכה לחקירות הונאה או מעילה בחברות מסחריות ובעסקים. במרבית המקרים פנייה למשטרה ללא ראיות משמעותיות תומכות תביא לסגירת התיק

לכן ברוב המקרים שבהם לא יומצאו עם התלונה ראיות משמעותיות תומכות, התיק ייסגר מחוסר עניין לציבור או מחוסר ראיות מספיקות, ולעיתים למרבה האבסורד גם מחוסר אשמה.

לסגירת התיק המשטרתי יש היבטים משמעותיים הן באפקט ההרתעה מול עובדי הארגון שבו אירעה המעילה או ההונאה והן בהליכים שיינקטו לאחר מכן לגביית הנזק מהמועל.

לפיכך הפנייה למשטרה צריכה להתבצע רק בשלבים מתקדמים, כאשר כבר יש דוח חקירה המגובה בראיות.

סיכום

התגלתה מעילה? ראוי ורצוי למנות משרד חקירות בעל ידע ומיומנות כדי לנהל את תהליך איסוף המידע המקדים וחקירת החשודים.

ביצוע חקירה ע"י גורמים מורשים ומוסמכים והכנת דוח חקירה שבו ראיות של ממש (שמוגש יחד עם התלונה למשטרה), מזרזים את הטיפול המשטרתי ומגדילים את סיכוי ההצלחה של ההליך הפלילי. ניתן יהיה להיעזר בדוח גם בהליך האזרחי להשבת סכום המעילה או ההונאה.

טיפול נכון ע"י גורמים מקצועיים הוא ההבדל בין הסיכוי להצלחת התהליך או לכישלונו.

בינה מלאכותית והמבקר הפנימי

מאת

רו"ח לינור דלומי | שותפה, ראש חטיבת ניהול הסיכונים, Deloitte

רן ברגמן | שותף ומדען נתונים ראשי, Deloitte

טכנולוגיה כמנוע שינוי בתהליכי קבלת החלטות

משחר קיומה של התרבות האנושית הייתה הטכנולוגיה מנוע שינוי רב עוצמה. הטכנולוגיה לא רק נתנה יתרון תחרותי לחברות ותרבויות, אלא גם שינתה את האופן שבו אנו תופסים את המציאות ומתייחסים אליה. גם כיום הסביבה העסקית והארגונית עוברת שינויים מרחיקי לכת, הנובעים מהתפתחות מואצת ביכולות הטכנולוגיות.

השינוי המהותי שמתרחש בימים אלו באימוץ טכנולוגיה, הוא שבנוסף על מיכון תהליכים עסקיים, אנו מתחילים למכן גם החלטות עסקיות

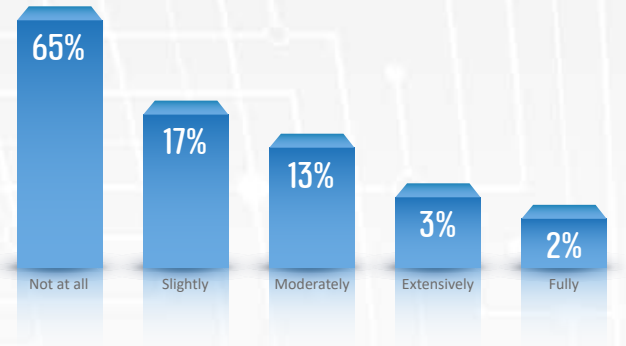
אנו כבר רגילים לכך שהטכנולוגיה הקיימת מאפשרת למכן תהליכים עסקיים שעד כה בוצעו רק באמצעות בני-אנוש. השינוי המהותי המתרחש בימים אלו הוא שאנו מתחילים למכן גם את תהליכי קבלת ההחלטות.

הדוגמה הפשוטה להפליא היא היישומון Waze (להלן - המכונה). מי מאיתנו לא עשה שימוש ביישומון זה? כאשר אנו מתקינים את היישומון לראשונה ומתחילים להשתמש בו, רובנו עושים זאת עם חשש מסוים. אנו למעשה חוששים מאיבוד השליטה והעברת האחריות למכונה. לכן רובנו נבחר לעשות זאת בהדרגה:

1. השימוש הראשון ביישומון ייעשה בדרך כלל כתהליך התומך בקבלת החלטות: "בוא נראה דרך איפה הוא ממליץ לנסוע". אנו לא מאבדים שליטה, אלא רק מבקשים מידע התומך בקבלת ההחלטה בנוגע למסלול הנסיעה.
2. בשלב השני, לאחר ביסוס אמון, ישנה העברה חלקית של תהליכי קבלת ההחלטות למכונה (שימוש במכונה עבור ניווט למקומות חדשים בלבד), או העברה לתפקיד הניטור והבקרה בבחינת "אני אנווט ונראה מה הוא אומר" (כלומר המכונה עובדת ברקע כסוג של תהליך בקרה על קבלת ההחלטות שלנו).
3. בשלב השלישי, אנו מרשים לעצמנו להעביר שליטה אל המכונה - לתת לה לקבל עבורנו את ההחלטות ולנווט אותנו ליעדנו באופן מלא ועצמאי.

ארגונים עוברים את תהליך אימוץ הטכנולוגיה באופן דומה. ישנם ארגונים המצויים בשלב 1, שבו הארגון מפעיל מערך דוחות כתמיכה בקבלת החלטות. רוב הארגונים כבר מצויים בשלב 2, שבו חלק מהתהליכים ממוכנים באופן מלא, לרבות קבלת החלטות ברמת מורכבות נמוכה. דוגמה לכך ניתן למצוא בתהליך אישור אוטומטי של רכישת פוליסת ביטוח או קבלת הלוואה. היכולת למכן את התהליך באופן מלא, לרבות קבלת ההחלטה האם לאשר או לא, כלומר שלב 3 בהתפתחות, כבר קיימת ופועלת בחלק מהארגונים.

בסקר של ה-IIA בדצמבר 2017 נשאלו הנסקרים באיזו מידה הארגון שלהם מפעיל בינה מלאכותית. מהסקר עולה כי 35% מהארגונים בצפון אמריקה ומערב אירופה מפעילים היום בינה מלאכותית בהיקף כלשהו.



לצד ההזדמנויות החדשות שמייצר השימוש בבינה מלאכותית, נוצרים גם סיכונים מסוג חדש למערכת הארגונית.

זהו תחום חדש שעדיין נמצא בהתהוות ולא ניתן להבין לגמרי את השלכותיו. מכיוון שלא נצבר ניסיון הולם, ארגונים טרם הטמיעו תורת הפעלה סדורה, לא קיימים מספיק מנגנוני בקרה, ואין תוכניות להתמודדות עם הסיכונים החדשים ועם הנזק שעלול להיווצר עם התממשותם.

כתוצאה מכך, נראה בשנים הקרובות יותר ויותר פעולות של רגולטורים וארגונים החותרים להסדרת התחום. במסגרת מאמץ זה, למבקר הפנימי יש תפקיד חשוב ומשמעותי במתן המענה: החל משלב בחינת נאותות היכולות המוצהרות של המערכת, דרך שלב היישום וההטמעה באופן נכון, וכלה בשימוש השוטף בבינה מלאכותית לצורכי הביקורת הפנימית.

מהי בינה מלאכותית?

ההגדרה המקובלת ביותר לבינה מלאכותית הוטבעה בשנת 1950 על ידי אלן טיורינג (האדם שעזר לפצח את מכונת ההצפנה של הנאצים במלחמת העולם השנייה - אניגמה), וידועה בשם מבחן טיורינג.

מכונה תיחשב לתבונית כאשר אדם היושב בחדר סגור ומנהל איתה שיחה לא יוכל לזהות שמדובר במכונה (או במחשב). נכון לשנים האחרונות, תוכנה הצליחה ב-33% מהמקרים לדמות שיחה ברמה אינטלקטואלית של נער בן 13 שנים (כדי לעבור את מבחן טיורינג נדרשת הצלחה ב-30% מהמקרים לפחות).

אנחנו עדיין לא קרובים למצב שבו מכונה מחליפה אדם, אבל הבינה המלאכותית מאפשרת לנו לתת מענה לבעיות פשוטות של קבלת החלטות.

להלן מספר דוגמאות מהמציאות שלנו:

1. מכוניות אוטונומיות.
2. קביעה אוטומטית של ציוני סיכון לאנשים (תביעות, חיתום, הלוואות, כניסה לניתוחים וכדומה).
3. התאמה אוטומטית ופרטנית של מסרים והצעות ערך בזמן אמת.
4. התאמה פרטנית של תרופות על בסיס מאפיינים קליניים של מטופל (ובהמשך על בסיס מבנה גנטי).
5. טייס אוטומטי במטוסי נוסעים.

בכל הדוגמאות הללו מכונה מקבלת החלטות עבורנו, ולא תמיד אנו מודעים לכך ובוודאי לא תמיד מבינים כיצד התהליך פועל.

נמחיש כיצד פועלת בינה מלאכותית על ידי דוגמה של בקרת חשבוניות. אנו רוצים לזהות באופן אוטומטי ומקוון האם ישנן חשבוניות חריגות, העשויות להצביע על נוהל לא תקין או "פרצה" (ליקוי) בנוהלי הבקרה המופעלים בארגון.

מודל

מטרתו של מודל סטטיסטי (סטוכסטי - תהליך אקראי שהתפתחותו תלויה בגורמים מקריים) היא הבנת הקשר בין אוסף מאפיינים של ישות.

בדוגמה שלנו, מאפייני חשבונית הם מספר חשבונית, ספק, יחידה ארגונית, מאשר, תאריך, מק"ט, כמות, סכום ועוד.

תוצאה או אינדיקטור לגבי חשבונית תהיה, למשל, האם החשבונית חריגה או לא.

מטרת המודל היא לאפשר "קבלת החלטה" בנוגע לכך שחשבונית מסוימת היא חריגה ויש צורך להתריע עליה.

אלגוריתם

הביטוי הפיזי של המודל הוא האלגוריתם, שהוא למעשה אוסף פעולות שהמכונה מבצעת על מנת לקבל "החלטה". על מנת לעשות זאת, המכונה "לומדת" מהנתונים הקיימים ו"בונה מודל" המתורגם לאלגוריתם. את האלגוריתם הזה המכונה תפעיל על כל חשבונית חדשה שתעבור במערכת.

האלגוריתם עשוי להיות למשל: "חשב לכל חשבונית את מידת המרחק מהממוצע כתלות בהשתייכות לאשכול ספקים. אם המרחק גדול משתי סטיות תקן, קבע כי החשבונית חריגה".

לכל אלגוריתם יש קלט הבנוי ממשתנים (מאפיינים) המכילים נתונים, ופלט הבנוי ממשתנה המכיל תוצאה.

בדוגמה שלנו, הקלט הוא מאפייני כל חשבונית, והפלט הוא האינדיקטור האם החשבונית חריגה.

"למידת מכונה" (MACHINE LEARNING)

כדי לבנות מודל, יש לקבוע ראשית אילו מאפיינים (משתנים) ייכללו בקלט.

למידת מכונה היא מצב שבו אנו לא בוחרים מראש אילו מאפיינים ייכללו בקלט. במקום זאת, המכונה "בוחרת" אותם באופן עצמאי על פי מנגנון שנקבע מראש.

למידת מכונה מאפשרת לנו לבנות את המודלים כל פעם מחדש, ביעילות גבוהה מאוד, ולהתאים את המודל למצבי מציאות משתנים. בדוגמה של החשבוניות, הוספת ספקים או יחידות ארגוניות לא תשנה את אופן פעולת המכונה. לאחר מספיק זמן (מספיק רשומות חדשות), המודל יותאם למצב החדש ללא התערבות.

ניתן לבצע "לימוד" מכונה בשני אופנים:

1. **לימוד מובנה (Supervised)** | כאשר יש לנו דוגמאות מהעבר שמהן ניתן ללמוד (בדוגמה שלנו: חשבוניות חריגות שכבר זוהו). המכונה מכלילה מתוך מקרי העבר את המודל ומחילה אותו על כלל המקרים.

2. **לימוד לא מובנה (Unsupervised)** | כאשר אין לנו דוגמאות מהעבר שמהן ניתן ללמוד, המכונה תקבץ מקרים דומים על פי מאפייניהם ותאתר מקרים שלכאורה היו אמורים להיות באותה קבוצה, אך מאפיין אחד או יותר הם חריגים לקבוצה. המכונה למעשה בונה את ה"תקן", ואז מזהה מקרים שאינם עומדים בו.

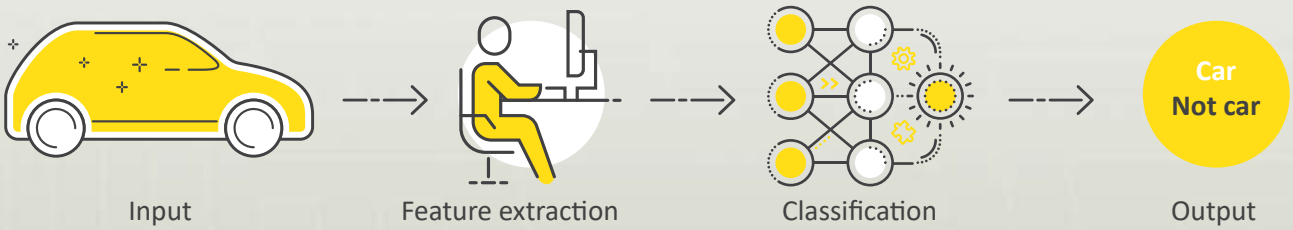
DEEP LEARNING

בשונה מלמידת מכונה שבה המכונה בוחרת מאפיינים בהתאם למנגנון שנקבע מראש מתוך רשימה קיימת של מאפיינים, "לימוד מעמיק" מייצג מצב שבו המכונה מחליטה ובוחרת מאפייני מודל ללא מנגנון שנקבע מראש. נניח כי אנו באים לבדוק פעילות חריגה של עובדי בנק באמצעות ניתוח טרנזקציות בנקאיות, או לבדוק נוהל רישום תרופות על ידי רופא למטופל באמצעות ניתוח כלל המרשמים הניתנים. כאן המורכבות נובעת מהצורך לייצר מאפיינים שאינם מצויים ברשומה המקורית. במקרה של טרנזקציות בנקאיות, אנו רוצים להגדיר מאפיין חדש המחשב את היחס בין הטרנזקציה האחרונה לבין הממוצע של עובד הבנק ביחידת זמן. השאלה היא כיצד להחליט כי זהו המאפיין שכדאי לנו לעשות בו שימוש. באופן דומה, ישנם אלפי או מאות אלפי מאפיינים אחרים שלא חשבנו עליהם.

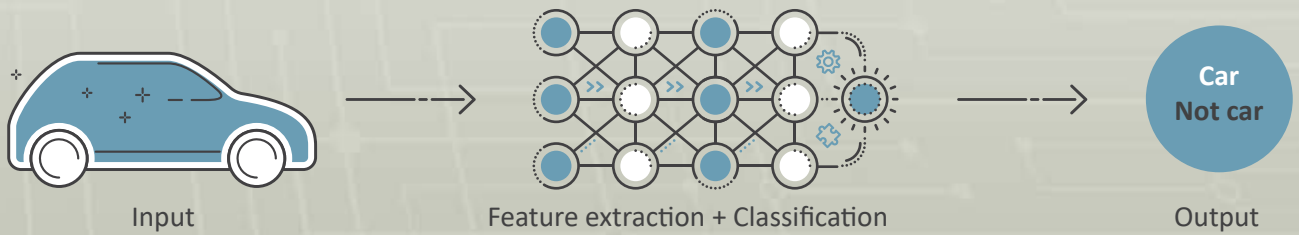
כאן נכנסת לתמונה יכולת ה-Deep Learning. במקרה זה, המכונה מייצרת באופן עצמאי את המאפיינים שהיא תבדוק לאחר מכן.

כיום הבינה המלאכותית מסוגלת לפעול על מאגרי נתונים המכילים מיליוני רשומות ועשרות אלפי מאפיינים הנוצרים באופן אוטומטי.

MACHINE LEARNING



DEEP LEARNING



סיכון בשימוש בבינה מלאכותית: טעות של המכונה

בבואנו להעריך את איכות "ההחלטה" של מכונה, צריך לבחון שני סוגים של טעויות:

טעות מסוג ראשון | המכונה החליטה על תשובה חיובית, אך בפועל טעתה. לדוגמה, מכונה קבעה כי הלקוח יקבל הלוואה, אך בפועל הלקוח לא שילם את ההחזר. כאן הנזק הוא ההפסד הכספי של חדלות הפירעון. דוגמה נוספת, מכונה קבעה כי מטופל יקבל אישור לתרופה אך בפועל התרופה פגעה במטופל. במקרה זה, מלבד הנזק הבריאותי והכספי, עלולה להיות גם פגיעה במוניטין בצורה של תביעת רשלנות רפואית.

טעות מסוג שני | המכונה לא החליטה על תשובה חיובית, אך בפועל הייתה צריכה להחליט. לדוגמה, המכונה קבעה כי הלקוח לא יקבל את ההלוואה, אך בפועל הלקוח היה משלם את ההחזר במלואו. במקרה זה הנזק הוא הפסד הכנסה.

כאשר אנו באים לאמוד את התרומה של השימוש בבינה מלאכותית, עלינו לשקול את היקפי הטעות מסוג ראשון ושני ולכמת את הנזק העלול להיגרם בכל מצב. רק הבנה מושכלת של מצבי הטעות והנזק בכל מצב, תאפשר לאמוד את הסיכון הקיים ולקבוע תוכנית להתמודדות עם הסיכון.

source: https://www.flickr.com/photos/jackson3/3733049190
http://www.yo-yoo.co.il/coolpics/images/uploads/dog33.jpg

ביקורת פנימית ובינה מלאכותית

בינה מלאכותית בעולם העסקי תשפיע על הביקורת הפנימית בשני אופנים:

1. השפעה על שיטות העבודה של יחידת הביקורת.
2. השפעה על המיומנויות הנדרשות על מנת לבצע ביקורת על תהליכים עסקיים שבהם נעשה שימוש בבינה מלאכותית.

השפעה על שיטות העבודה של הביקורת הפנימית:

לאור התגברות האתגרים ומורכבות הפעילות העסקית והלחץ על התייעלות כלכלית, האתגרים העומדים בפני פונקציית הביקורת הפנימית כוללים התמודדות עם מורכבות גוברת זו במשאבים מועטים:

"Doing more with less"

רתימת טכנולוגיה, ושימוש בבינה מלאכותית בלבד, מאפשרת ליישב את הצורך בהגברת האפקטיביות ושיפור יכולות הביקורת בד בבד עם התייעלות וחיסכון במשאבים בראייה ארוכת טווח.

התייעלות בתהליכי עבודה: הביקורת הפנימית תעשה שימוש הולך וגובר ביכולות מעולם הבינה המלאכותית כחלק אינטגרלי מארגז הכלים שלה. **השימוש בבינה מלאכותית יכול לשפר את עבודת המבקר הפנימי ולייעל אותה.**

בינה מלאכותית מאפשרת לביקורת הפנימית לזהות כשלים שעד היום לא ניתן היה לזהות, לכסות יותר "שטחים", ולבצע זאת בפחות זמן ומשאבים. כל זאת, ללא פגיעה באיכות העבודה (לפעמים אף בשיפור).

התייעלות נוספת תתאפשר על ידי יצירת תהליכי ביקורת שחוזרים על עצמם באופן אוטומטי. לדוגמה, ביקורת שכר תתבצע אחת למספר חודשים במקום אחת למספר שנים. ההשקעה בביקורת מבוצעת פעם אחת, ומכאן התהליך הוא אוטומטי ולומד.

כיום, בעזרת בינה מלאכותית אנו יודעים לבצע ביקורות על כלל נתוני מערכת ארגונית בשבועות בודדים, תוך צמצום למינימום של פרק הזמן שבין שליפת הנתונים ועד העברת התובנות.

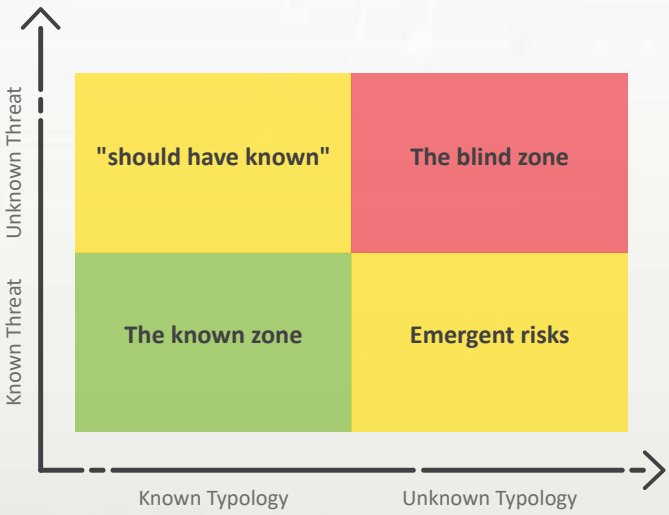
שינוי צורת עבודה: הביקורת הפנימית תתחיל לעבוד עם בינה מלאכותית כדי לזהות כשלים פוטנציאליים (חריגים או "אנומליות"), בלי להגדיר מראש "מה מחפשים".

כיום, זיהוי מצבי כשל מתחיל בהגדרה מוקדמת של מצב הכשל הפוטנציאלי ואיתור של מצב זה בהתנהלות השוטפת. לרוב מדובר בהשוואה של התנהלות קיימת מול פרוטוקול או תקן התנהגות רצוי.

בינה מלאכותית מאפשרת לביקורת הפנימית לזהות מצבי קיצון, חריגה ואי התאמה שלא הוגדרו מראש.

בכך נפתח עולם חדש ואינסופי של מצבים שעד כה לא היו מטופלים. יש לזכור כמובן את הטעות מהסוג הראשון: מצבים קיצוניים, חריגים או לא מתאימים שהם בכל זאת תקינים. למשל, משכורת חריגה אינה מצביעה בהכרח על חוסר תקינות, מפני שייתכן שהיא מבטאת בונוס חד-פעמי שאושר באופן תקין.

טבלת מיפוי הסיכונים הארגוני



"The Known Zone" - אופן העבודה הנוכחי, שבו המבקר הפנימי עוסק בסיכונים ידועים ובטיפולוגיה ידועה. הסיכון ידוע ואופן זיהוי הכשל ידוע. זה האופן שבו אנו פועלים ללא בינה מלאכותית.

"Should Have Known" - הסיכון לא ידוע, אך הטיפולוגיה ידועה. במקרה זה ניתן לזהות חריגה מהסטנדרט ללא ידיעה מקדימה בדבר התקינות של האירוע. לדוגמה, חשבונית חריגה לפי מודל ידוע מראש. במקרה כזה המכונה מפעילה שיקול דעת כדי לקבוע האם רשומה במערכת היא חריגה ומצריכה תחקור מעמיק יותר.

"Emergent risk" - הסיכון ידוע אך לא קיים מנגנון זיהוי הכשל. במקרה כזה הבינה המלאכותית מאפשרת לנו לזהות תבניות התנהגות העשויות לרמז על כשלים במקרים של סיכונים ידועים ללא הגדרה מראש של הכשל. לדוגמה, ריבוי פתיחת חשבונות ממדינה זרה, העשוי לרמוז על פעילות הלבנת הון.

השפעה על המיומנויות הנדרשות על מנת לבצע ביקורת על תהליכים עסקיים שבהם נעשה שימוש בבינה מלאכותית:

ההטמעה של בינה מלאכותית בתהליכים עסקיים בארגון תיצור תפקידים חדשים וצורך בבחינת יכולות שונות לצוות הביקורת הפנימית.

המבקר הפנימי יצטרך לבקר את האופן שבו הארגון מפתח ועושה שימוש בבינה מלאכותית. לשם כך, יחידת הביקורת הפנימית תידרש להשלים ידע, להעלות את נושא הבינה המלאכותית בוועדת הביקורת, ולגבש תוכניות התמודדות עם הנושא.

השפעה על תוכנית העבודה ונושאי בדיקה במטרה לכלול זיהוי סיכונים בתהליכים עסקיים הכוללים בינה מלאכותית:

הטמעת יכולות בינה מלאכותית בארגון מייצרת סיכונים שעל הביקורת הפנימית לבחון בתהליך הביקורת, לדוגמה:

1. **סיכון הגורם האנושי** - למרות שאנו מפעילים מכונה על מנת לקבל החלטות, בסופו של דבר עדיין בן אנוש מתכנת ומטמיע את האלגוריתם. בניגוד לטיפול במערכות מידע, לרוב אין בארגון את אותם מנגנוני בקרה על מדעני הנתונים. לכן אנו יכולים לזהות מספר סיכונים בתהליך:
   - הטיות אנושיות לא מזוהות המשולבות באלגוריתם.
   - טעויות לוגיות אנושיות באלגוריתם.
   - תהליך לא מספק של העברה לייצור, בדומה לפרוטוקולים הקיימים במערכות מידע.
2. **השלכות אתיות של הפעלת האלגוריתם** - לדוגמה, האם האלגוריתם אכן לא מפלה בין קבוצות אתניות, למרות שהן יוצאות מובחנות?
3. **הסיכון בגרימת נזק** - מוצרים או שירותים מבוססי בינה מלאכותית עלולים לגרום נזק פיננסי או נזק למוניטין.
4. **הסיכון כי הארגון או יחידות עסקיות לא ישכילו להטמיע** ולעשות שימוש ביכולות בינה מלאכותית ובכך יסכנו את הארגון כולו.
5. **הסיכון כי עקב חוסר ידע, הבנה או יכולת,** הארגון לא ינצל כראוי את ההשקעה המסיבית המושקעת בהטמעה של יכולות בינה מלאכותית ואף יגיע לאי החזר על ההשקעה.

אילו נושאים המבקר צריך לכלול בתוכנית העבודה לגבי בינה מלאכותית?

1. בדומה לשימוש בכל מערכת מרכזית אחרת, על הביקורת הפנימית לוודא שימוש ראוי בבינה מלאכותית בהיבטים הבאים:

   - **ממשל תאגידי (Corporate Governance)** - אילו מדיניות ונהלים יש לקבוע כדי להבטיח ממשל תקין? האם מסגרות הניהול הקיימות פועלות? מי בודק האם ליחידות העסקיות יש הכישורים הנדרשים והמומחיות לנטר ולפקח על פעילות הבינה המלאכותית? כיצד הארגון מוודא כי הערכים שלו והאתיקה שלו משתקפים בפעילות הבינה המלאכותית? האם האסטרטגיה העסקית כוללת פיתוח יכולות בינה מלאכותית וכישורים מספקים על מנת להפיק ערך מיכולות אלה למימוש האסטרטגיה?
   - **ממשל נתונים (Data Governance)** - בארגונים שבהם יש מבנה מוגדר היטב וקוהרנטי של הנתונים, יש לבחון האם היחידות העסקיות המפתחות, מטמיעות ועושות שימוש בבינה מלאכותית אכן מפעילות מנגנוני בקרה על איכות הנתונים? אנו יודעים לזהות כיום מספר מצבי פגיעה באיכות הנתונים העלולים להשפיע לרעה על הפעלת אלגוריתם של בינה מלאכותית (לדוגמה: שלמות, דיוק, תאימות, רציפות, תקפות, עדכניות, מהימנות ועקביות).
   - **ניהול סיכונים** - האם ישנם מנגנונים המבטיחים כי לא ניתן לעשות שימוש לרעה בבינה המלאכותית על ידי גורמים מחוץ לארגון או בתוכו?
   - **תהליכים סדורים** להטמעת יכולות בינה מלאכותית (כגון פרוטוקולים של העברה לייצור של בינה מלאכותית).

2. סיכונים הנובעים מפעילויות בינה מלאכותית - הערכת הסיכון, ושילובו בתוכנית הביקורת השנתית, בהתאם להיקף ומהותיות הפעלת יכולות מסוג זה.

3. הביקורת הפנימית צריכה להיות מעורבת באופן פעיל בפרויקטים של בינה מלאכותית מהשלב הראשון. המעורבות תתקיים במתן ייעוץ מקצועי במטרה לתרום ליישום מוצלח, כמובן בלי לקחת חלק בתהליך קבלת ההחלטות ובלי לפגוע בעצמאות ובאובייקטיביות של המבקר.

4. בארגונים שכבר מיישמים היבטי בינה מלאכותית (כגון ייצור באמצעות רובוטיקה בקו הייצור) או משלבים אותה במוצר או בשירות (כגון התאמה אישית של הצעות ערך על בסיס היסטורית רכישה), הביקורת הפנימית צריכה לבחון, כחלק מתהליכי הביקורת, את ההיבטים הקשורים באמינות של האלגוריתמים הבסיסיים והנתונים שעליהם מבוססים האלגוריתמים.

5. הביקורת הפנימית צריכה לבחון את ההיבטים האתיים בשימוש בבינה מלאכותית, וכחלק מביצוע הביקורת לבחון עמידה בהיבטים האתיים הללו.

6. הביקורת הפנימית תפעל לבחון תהליכי קבלת החלטות המתבצעות על ידי מכונות. לדוגמה, כיצד בוחנים את תהליך חסימת כרטיס אשראי, כאשר הוא מתבצע באופן אוטומטי ומבוזר תוך שילוב מספר מכונות המפעילות "שיקול דעת".

סיכום

תחום הבינה המלאכותית כאן כדי להישאר. התחום מביא עמו יכולות חדשות בתחום העסקי שיאפשרו התייעלות ושיפור ביצועים ואפילו התפתחות של מודלים עסקיים חדשים. בד בבד, התחום מביא איתו אתגרים חדשים בתחום הביקורת הפנימית וניהול הסיכונים.

תחום זה הוא אחד הפתרונות המרכזיים לאתגרי הביקורת, הכוללים עלייה במורכבות הפעילות העסקית והדרישות מהביקורת הפנימית, ולחץ מתמיד להתייעלות ולחיסכון במשאבים. על הביקורת הפנימית להשתמש בכלים החדשים שמביאה הבינה המלאכותית כדי להתייעל ולהשתפר, ובמקביל לסייע בשמירה על הארגון מפני הסיכונים הנובעים משימוש בכלים אלו.

תחום זה הוא תחום חדש שעדיין לא נחקר דיו, ובשנים הקרובות יהיה צורך לבנות עבורו מסגרות עבודה וקווים מנחים.

תוכנית אקטיבית לצמצום חשיפות להונאות ומעילות

לבטים ומיטב התובנות האישיות שלי

מאת

רחלי בן משה | רו"ח, CIA, מבקרת פנימית רכבת ישראל

מיידוף, מכירים? לא מזמן קראתי מאמר שמנתח את ההונאה הגדולה בשוק ההון האמריקאי. הכותב, מבקר פנימי במקצועו, סיכם את המאמר במסקנה כי סביר שמינוי מבקר פנימי בלתי תלוי שמדווח לוועדת ביקורת עצמאית, היה חושף את ההונאה וחוסך אובדן כספי גדול.

אני אמנם לא מכירה את פרטי הפעולה של מיידוף ושל הארגון בבעלותו כפי שאותו כותב מכיר, אבל אני זוכרת שהסיכום שלו טרד את מנוחתי. אני עוסקת בביקורת פנימית וכיהנתי כמבקרת פנימית בארגונים שונים במשך מרבית שנותיי המקצועיות. בין היתר, הייתי המבקרת הפנימית של הראל פיננסים, אחרי המעילה. את התוספת הזו, "אחרי המעילה", אני מוסיפה בצורה אוטומטית בכל פעם שאני מציגה את עצמי. התוספת האוטומטית הזו מקפלת בחובה משמעות גדולה - לא הייתי שם באותה תקופה, אל תחברו אותי לסיפור הזה. אבל האם התוספת האוטומטית הזו גם אומרת גם "לי זה לא היה קורה..."? אני לא בטוחה.

במהלך השנים פגשתי כל כך הרבה מנהלים שאמרו "לי זה לא יקרה".
אני הפסקתי לנסות ולרמות את עצמי.

ייתכן שמעילה בהיקף כל כך גדול כמו שביצע מיידוף לא הייתה מתרחשת, אבל אני לא מוכנה לשבת בכיסא של אותו מנהל שבטוח שלו זה לא יקרה. מבקר פנימי זה תפקיד מאתגר, וישנם דברים רבים שטורדים את מנוחתו. כל מבקר פנימי הוא אחר, כל אחד רואה את הדברים דרך המשקפיים שלו וכל אחד מביא עמו עולם דגשים משלו. אני באופן אישי יכולה לא להירדם בלילה בשל החשש לא רק ממעילה בהיקף גדול ומשמעותי בחברה שבה אני מבקרת, אלא גם בשל החשש מגילוי מעילה קטנה יחסית בתחום פעילות שבו בוצעה לאחרונה ביקורת פנימית שלא גילתה את המעילה. כל זאת אף שעל פי התקנים המקצועיים שיפורטו להלן אין באחריות המבקר הפנימי להיות מומחה לגילוי מעילות.
ולמי שנשאר ער בלילה, יש זמן לחשוב ולתכנן.

מידע כללי על התממשות הסיכון וכלים לניהולו

איגוד בוחני ההונאות (ACFE Association of Certified Fraud Examiners) מפרסם אחת לתקופה סקר בינלאומי שסוקר מקרי הונאה ומעילה מרחבי העולם. נתוני הארגון מצביעים על ממוצע נזק לחברות כתוצאה ממעילות והונאות של כ-5% מהמחזור השנתי. ממצאי הסקר מצביעים על כך שהמקרים הרבים ביותר מתבצעים בנכסי החברה, אולם הנזק המצטבר שלהם נמוך יחסית. בצד השני של הספקטרום נמצאים מקרי הונאות בדיווח הכספי, שהם אמנם מועטים יחסית במספרם אבל בעלי היקף הנזק הגדול ביותר.

עוד עולה מהסקר, כי הדרך הנפוצה ביותר לגילוי מעילה (כ-40% ממקרי המעילה) הייתה מידע שהתקבל או הלשנה. כפועל יוצא, הסבירות לאיתור מעילה קיימת גבוהה יותר בארגונים שבהם הוטמע קו חם מאשר באלו שלא.

ארגון שרוצה להתחיל לטפל בנושא ולא יודע היכן להתחיל, צריך להתחיל באבחון אישי של מצבו.

כלי אבחון נמצאים ברשת, ואחד מהם מפורסם על ידי איגוד בוחני ההונאות. באתר האינטרנט של האיגוד תוכלו למצוא שאלון שמאפשר למנהל בארגון למפות היכן הארגון שלו נמצא ביחס לתהליכי ניהול הסיכון להונאות ומעילות. השאלון עוסק בנושאי אחריות, מדיניות, הערכת סיכונים, תהליכי בקרה, אמצעים לצמצום חשיפה ברמת תהליכים, אמצעים ברמת חברה (קוד אתי, תרבות ארגונית, תקשורת ארגונית), זיהוי פרואקטיבי של מעשי מרמה ואופן הטיפול בהם.

סטנדרטים מקצועיים ומודלים מקובלים

התקנים המקצועיים הבילאומיים של ה-IIA מנחים כי פעילות הביקורת הפנימית תעריך את הפוטנציאל להתרחשות של הונאה ואת האופן שבו הארגון מנהל את הסיכון (A2.2120),

תוכנית מובנית למניעת מעילות מקרינה לעובדים נחישות של ההנהלה ומעניקה תחושת ביטחון להנהלה הבכירה ולדירקטוריון.

וכן שלמבקר פנימי יהיה ידע מספק כדי להעריך את הסיכון להונאה ואת האופן שבו הסיכון מנוהל. עם זאת, אין לצפות מהם להיות בעלי ההתמחויות של מי שתפקידו העיקרי הוא לגלות ולחקור הונאות (A2.1210). בנוסף, הנחיה GTAG 13 של ה-IIA בנושא "מניעת הונאות ואיתורן בעולם הטכנולוגי" מתייחסת למתודולוגיה לאיתור הונאות והשימוש בכלים טכנולוגיים להשגת מטרה זו. בארגונים שמיישמים SOX קיימת התייחסות לניהול סיכוני הונאות ומעילות.

כמו כן, בספטמבר 2016 פרסם ארגון COSO (Committee of Sponsoring Organizations of the Treadway Commission) את המדריך שלו לניהול סיכוני הונאות. המדריך מתייחס לאבני דרך ליישום תוכנית לניהול סיכוני הונאות, וכולל מדיניות ניהול וממשל סיכוני הונאות, הערכת הסיכונים, תכנון ויישום פעילויות בקרה מונעות ומגלות, ביצוע חקירות והמשך ניטור והערכת הסיכון. **האם זו אחריותו של מבקר פנימי? האם מבקר פנימי נדרש להיות אקטיבי בנושא הזה?**

התקנים המקצועיים קובעים במפורש שלא, אך לא פעם השינה של המבקר הפנימי נודדת בלילה בשל הדברים הללו. גם אני מוטרדת מכך, ובאופן אישי אני סבורה שאם זה מפריע לי לישון אז אני צריכה לטפל בזה.

התוכנית שיישמנו ברכבת ישראל

ניסיתי לפתוח את ה-text book. לא מצאתי מודל אחד שניתן לקחת וליישם בשיטת "גזור הדבק". בשנת 2015 זכיתי להשתתף בתוכנית מנהיגות בינלאומית שבמסגרתה התדפקתי על דלתם של מבקרים פנימיים רבים ברחבי ארה"ב. גיליתי את מה שכבר ידעתי קודם, כל מבקר מטפל אחרת בנושא, כל אחד רואה את אחריותו ובהתאם את הנדרש ממנו במשקפיים הפרטיים שלו. פגשתי מבקרים (רבים) שמתייחסים לנושא מעילות והונאות כאל עוד אחד מסיכוני הארגון, ובארגונים שבהם פונקציות ניהול סיכונים לא קיימות, גם הסיכונים הללו אינם מנוטרים באופן שוטף אלא נלקחים בחשבון במסגרת ביקורות פנימיות בנושאים ספציפיים. בקוטב האחר של הסקאלה פגשתי מבקרים פנימיים (מעטים) שהחליטו לא להמתין לפונקציית ניהול הסיכונים ולטפל בצורה אקטיבית בנושא. הטיפול הזה כלל בעיקר ביצוע סקר סיכוני הונאות ומעילות ומיסוד קו חם.

אחת הסברות המעציבות היא שרוב הארגונים מתחילים לטפל בנושא רק לאחר שחוו אירוע של מעילה. כשחזרתי לארץ חקרתי בקצרה את הנושא

והתחלנו לתכנן וליישם ברכבת ישראל תוכנית אקטיבית לצמצום חשיפות להונאות ומעילות. אמנם הביקורת הפנימית הובילה את הקמת התוכנית, אולם המשימה לא יכולה להישאר בגבולות הביקורת.

מדובר במשימה משותפת של פונקציית ניהול הסיכונים (קודם כל) יחד עם שאר שומרי הסף, תוך שיתוף כלל ההנהלה.

ברור לכולם, וגם לי, שלא ניתן למגר לחלוטין את הסיכון. אי אפשר להגיע לחסימה מלאה של האפשרות לבצע מעילה בארגון. עם זאת, תוכנית מובנית למניעת מעילות מקרינה לעובדים נחישות של ההנהלה ומעניקה תחושת ביטחון להנהלה הבכירה ולדירקטוריון.

מטרות התוכנית

- הקטנת נזקים כלכליים, תפעוליים, משפטיים ותדמיתיים.
- זיהוי ומיפוי חשיפות לצד בחינה שוטפת של הבקרות.
- מיקוד לגבי הפניית משאבים לחיזוק מערך הבקרה הפנימית.

להלן האלמנטים העיקריים של התוכנית:

יצירת אווירה ארגונית	מיפוי סיכונים	ביצוע בקרות	בחינת חריגים	תוכנית אכיפה	ניטור ומעקב
פורומים להגברת מודעות	סקר סיכוני הונאות ומעילות	ניטור ביצוע בקרות מובנות קיימות	דוחות חכמים לאיתור חריגים	מדיניות ונהלים	עדכון תקופתי של רכיבי התוכנית
הגדרת כללי התנהגות	מיפוי תפקידים רגישים	ביצוע בקרות פתע מדגמיות	מערכות ממוחשבות BI	הגדרת ממשקים עם גורמים רלוונטיים	בחינה שוטפת של הבקרות
פורום שומרי סף	עיגון בקרות ייעודיות			דיווחים	"ביזם" תרחישי מעילה

חשוב להבין שאת בניית המערך ברכבת ישראל עשינו עוד לפני פרסום המדריך לניהול סיכוני הונאות של ארגון COSO (ספטמבר 2016). עם זאת, ניתן בהחלט לזהות את הרכיבים שהתייחסנו אליהם ברכבת גם במדריך COSO, המתייחס לאבני דרך ליישום תוכנית לניהול סיכוני הונאות - מדיניות ניהול וממשל סיכוני הונאות, הערכת הסיכונים, תכנון ויישום פעילויות בקרה מונעות ומגלות, ביצוע חקירות והמשך ניטור והערכת הסיכון. עם פרסום המדריך, וידאנו שהתוכנית שלנו תואמת וכוללת את רכיבי המודל כאמור.

יצירת אווירה ארגונית תומכת מהווה אתגר מרכזי בתוכנית

סיכום ביניים

האלמנטים השונים של התוכנית שלובים זה בזה ולא ניתן להעמיד אותם בסדר קשיח כלשהו (סדר כרונולוגי או סדר חשיבות). עם זאת, התוכנית שבנינו יושמה באופן מדורג.

האלמנט שמהווה אתגר עיקרי הוא יצירת אווירה ארגונית. יש לטפל במודעות של כלל המנהלים ומנהלי הביניים לנושא, וכן של גורמים רלוונטיים נוספים כגון אנשי משאבי אנוש, רכש, כספים ומערכות מידע.

מיפוי הסיכונים מצריך עבודה ראשונית מאומצת של מיפוי פעילויות, זיהוי תרחישי סיכון והערכתם.

על בסיסו של מיפוי הסיכונים נדרש לעגן בקרות ייעודיות שחלקן נגזרות ישירות מהמלצות הסקר וחלקן נבנות כחלק מביקורת מתמשכת.

מדריך COSO, שעליו ארחיב במאמרים הבאים, משמש בבחינת חליפה ליתום. כל אחד מהאלמנטים הללו מצריך חשיבה מובנית ותפירה למידותיו של הארגון הספציפי ועל כל אחד מהרכיבים הללו ניתן לפרט עוד. בחוויה האישית שלי, מצאתי שנכון יותר להתחיל בשלושת הרכיבים הראשונים (אווירה ארגונית, מיפוי סיכונים, עיגון בקרות) ולהגיע לשלב הרכיבים הנוספים רק כאשר הבסיס הזה כבר הונח.

כאמור, בקרות ייעודיות יכללו בין היתר כלים ודוחות מובנים לזיהוי והצפת חריגים. בימים אלו אנחנו בשלבי בחינה ורכש של מערכת לביקורת מתמשכת שתנהל באופן מובנה את הבקרות וזיהוי החריגים שנעשה בשלב זה על ידי בקר ייעודי שגויס לטובת העניין.

תוכנית האכיפה אליה אני מתייחסת, לוקחת את כלל מרכיבי התוכנית המוזכרים לעיל ומייצרת מדיניות, נהלים ותבניות דיווח. כל ניסיון קודם שלנו להסדיר את הנושא לפני ששלושת הרכיבים הראשונים הושלמו (אפילו חלקית) לא צלח, מפני שהמסמכים פירטו תהליכים תיאורטיים שהיה קושי ליצוק תוכן לתוכם.

ואחרי הכול, כמו בכל תוכנית לניהול סיכונים, המבנה חייב להיות מעגלי וחוזר על עצמו - ניטור ומעקב ועדכון לפי הצורך מותירים את התוכנית הזו רלוונטית, חיה ונושמת בארגון.

בסדרת המאמרים בגיליונות הקרובים נסקור בהרחבה כל אחד מהאלמנטים השונים של התוכנית.

Women in Internal Audit Leadership Forum

Oct. 3, 2018

Renaissance Downtown DC / Washington, D.C

פרצה קוראת לגנב – האם ואיך ניתן למנוע זאת?

לקחים ורשמים ממעילה בחברה מובילה בישראל

מאת

אייל בן אבי | רו"ח (משפטן) MBA, שותף ראש קבוצת ניהול סיכונים ו-Forensic ב-PwC Israel

אורטל ביגלמן | רו"ח, מנהלת מחלקת Forensic Accounting ב-PwC Israel

סקר הפשיעה הכלכלית הגלובלי לשנת 2018, שנערך על ידי PWC בקרב למעלה מ-7,200 חברות מ-123 מדינות ולראשונה גם מישראל, מצא כי 49% מהחברות חוו פשיעה כלכלית. אחת משלוש המעילות הנפוצות שחוו המשיבים הישראלים היא מעילה בתחום הרכש, אזור סיכון מהנפוצים ביותר בהיסטוריית המעילות בארץ ובעולם.

הניסיון מלמד כי מעילות בתחום הרכש מתרחשות במשך מספר שנים עד לחשיפתן (אם בכלל).

ממחקרים שנערכו בנושא עולה כי מעילות חד פעמיות ו/או קצרות מועד הן דבר חריג, שכן הסיפוק, הריגוש והתועלת יגרמו למועל לחזור שוב ושוב על הפעולה מתוך הנחה שלא ייתפס.

משולש המעילה מתאר שלושה גורמים הנמצאים בכל מצב של מעילה או הונאה ומייצרים את הפוטנציאל להתממשותו של סיכון למעילות והונאות: מניע, הזדמנות והצדקה.

מהמשיבים לסקר הפשיעה הכלכלית הגלובלי דירגו את גורם ההזדמנות כגורם העיקרי שעלול להביא להתרחשות של מעילה ו/או הונאה.

ההזדמנות היא למעשה המצב היחיד שעליו אנו כגורמי הבקרה בחברה יכולים להשפיע, היות שפרצה בבקרה היא פתח להתרחשות מעילה ו/או הונאה.

סקר מעילות והונאות

כמחצית מהחברות שהשתתפו בסקר הפשיעה הכלכלית עורכות מדי תקופה סקר מעילות והונאות במטרה לאתר פרצות בתהליכים העלולים להביא להתרחשות של מעילה ו/או הונאה בחברה. על הסקר לכלול את הפעולות הבאות:

- איתור מוקדי סיכון למעילות והונאות בחברה, כאשר כל מוקד סיכון מכיל תרחישים אפשריים לביצוע מעילה או הונאה.
- בחינת מסגרת הבקרה בכל אחד ממוקדי הסיכון שזוהו.
- ניתוח נתונים במטרה לזהות אנומליות.
- ניתוח והערכת הסיכון השיורי להתרחשות מעילה או הונאה במוקדי הסיכון שזוהו.
- גיבוש המלצות לחיזוק מסגרת העבודה לניהול הסיכון.
- בניית תוכנית לצמצום החשיפות שזוהו בתהליכי החברה.

מעילות בעולמות הרכש

תהליכי רכש מתנהלים באופן שונה מחברה לחברה, בין אם בעקבות גודל החברה, כמות הפריטים הנרכשים, היקפי העסקאות, תיאבון החברה לסיכון ועוד.

תהליך הרכש ברובו בנוי לפי השלבים הבאים:

הסיכון כי תתרחש מעילה בכל אחד משלבי תהליך הרכש קיים ואינהרנטי, בין אם התהליך הוא שולי ואינו מוסדר ובין אם הוא מבוקר ומאורגן.

לרוב, הוצאות הרכש בחברה הן בסכומים מהותיים ומהוות את עיקר הוצאות החברה. על כן, ובהיותו אזור סיכון מהנפוצים בהיסטוריית המעילות, קיימת רגישות רבה וחשיפה לפעולות בלתי מורשות בתהליך זה יותר מכל שאר התהליכים המתקיימים בחברה. מכאן שיש חשיבות רבה למפות את החשיפות האפשריות ולהתאים את מערכי הבקרה השונים לפוטנציאל הסיכון.

דוגמה מהשנים האחרונות היא מעילת ענק שהתגלתה בחברה מובילה בתחומה בארץ, שבוצעה על ידי מנהלת חשבונות שעבדה בחברה מיום הקמתה ונחשבה לעובדת מצטיינת, מסורה ואהודה על חבריה לעבודה.

אז כיצד בוצעה המעילה בפועל, אילו גורמי בקרה היו חסרים, מהן הבקרות הדרושות ואלו מהן היו מונעות את המעילה?

שיטת המעילה

על פי כתב האישום שהתפרסם, מנהלת החשבונות בחברה פתחה חשבון בנק על שם נעוריה והוסיפה לו מספר מילים המרמזות על ספק הפועל בתחום ההפקה. במשך כחמש שנים שינתה ללא ידיעת החברה את שמם של חלק מספקי החברה שאינם פעילים ובעלי יתרות זכות לשם הספק שהוסיפה לחשבונה האישי, איפסה את יתרות הזכות הכספיות של ספקים אלה והעבירה אותם לחשבונה האישי. מנהלת החשבונות הפקידה בתקופה זו המחאות של החברה לחשבונה הפרטי בסכום של מעל 10 מיליון ש"ח.

לאחר שמעילה זו צלחה במשך כחמש שנים, היא נקטה צעד נוסף והקימה במערכות החברה ספק פיקטיבי הזהה לשם החשבון הבדוי שפתחה. היא ביצעה רישום כוזב של פקודות במערכת הנהלת החשבונות של החברה, והפיקה המחאות לטובת הספק הפיקטיבי שהקימה. את חתימות שני מורשי החתימה על ההמחאות היא זייפה.

בשיטה זו הפיקה עשרות רבות של המחאות מזויפות לפקודת הספק הפיקטיבי (בסכום של מעל 14 מיליון ש"ח), את ההמחאות הפקידה בחשבון המרמה ומשכה משם כספים לשימושה האישי. את התהיות בנוגע לבגדיה היקרים ולרמת החיים הגבוהה, שהפגינה ביחס לבעלי שכר דומה בחברה, פטרה בטענה, כי בעלה העצמאי נהנה מהכנסות גבוהות. היקף המעילה הכולל הוערך במעל 24 מיליון ש"ח במשך יותר מ-10 שנים.

המעילה התגלתה במקרה על ידי חשבת החברה. כחודש לאחר חזרתה של מנהלת החשבונות מחופשת לידה, חשבת החברה איתרה רישום שנראה לה חריג ופנתה למנהלת החשבונות בבקשה לקבלת הסבר. מנהלת החשבונות הגיבה בצורה מתחמקת ולחוצה ומיהרה להסתלק מהחברה. האמור עורר את חשד החברה והוביל לחקירת המקרה.

כשלים בסביבת הבקרה

כיצד נגנב סכום עצום של כסף בלי שאנשי מערך הבקרה והכספים בחברה יחשדו בדבר? היכן היו שומרי הסף בחברה? היו כשלים רבים בסביבת הבקרה, והבולטים ביותר הם:

- לא הייתה הפרדת תפקידים נאותה בין הגורם המורשה להקמת ספק לבין הגורם המורשה להנפיק תשלום לספק.
- לא נעשתה בקרה אחר כרטיסי ספק שאינם ביתרת זכות, ולא נעשתה בקרה לבדיקת התאמה בין הרשום בכרטיסי ספק פעילים לתשלומים שהועברו בפועל לטובת הספק.
- סעיף הרכש בחברה המדוברת הוא מהותי, על כן קיים קושי באיתור חריגים באמצעות בדיקות ידניות. החברה לא עשתה שימוש בכלי ניתוח נתונים מתקדמים לצורך ניתוח פקודות יומן חריגות, איתור כפילויות, איתור פערים ברציפות שיקים, ופקודות יומן והצלבות שונות בין בסיסי נתונים. סביר שניתוח נתונים במטרה לאתר אנומליות היה מציף את הפערים בשלב מוקדם.

בקרות שיכלו למנוע את המעילה

מעילה זו הייתה יכולה להימנע על ידי קיומן של הבקרות הבאות:

- **בעת הקמת ספק חדש במערכת הנהלת החשבונות יידרשו אישורים של שני גורמים לפחות.** בקרה זו מיושמת כיום בחברות רבות בישראל, כאשר גורם אחד אחראי על הקמת הספק והזנת נתוניו למערכת, והגורם השני אחראי על הזנת פרטי חשבון הבנק של הספק וכן על בחינת אמיתות הנתונים שהוקלדו על ידי הגורם הראשון.
- **פתיחת ספק חייבת להיות מגובה במסמך פתיחת ספק, וכן בתעודת התאגדות ו/או אישור ניכוי מס ו/או אישור ניהול ספרים של הספק.** בקרה זו תפחית את האפשרות כי יוקם במערכות החברה ספק פיקטיבי. אמנם לא כל ספק שיש לו מסמכי התאגדות הוא בהכרח ספק של החברה, אך בקרה זו תקשה על גורם בחברה להקים ספק פיקטיבי.
- **בעת הקמת ספק יש לקבל מהספק מסמך רשמי מהבנק, כדוגמת דף חשבון או שיק מבוטל.** בקרה זו תוכיח לחברה כי חשבון הבנק שביקש הספק להעביר אליו את התשלומים המגיעים לו הוא חשבון הבנק של הספק.
- **בחינת תקינות ונכונות מספר העוסק מורשה או ח"פ של החברה.** בבקרה זו נבחן כי מספר העוסק מורשה/ח"פ שסיפק הספק לחברה הוא אמיתי ותואם לשמו של הספק.
- **הפרדת תפקידים בין הגורם שאחראי על הקמת ספק לבין הגורם שאחראי להעביר את התשלום לספק.** בקרה זו הכרחית ומייצרת הפרדת תפקידים נאותה המונעת אפשרות כי עובד יחיד יבצע את הליך יצירת ההתקשרות עם הספק והזרמת התשלום לחשבונו ללא מעורבות גורמים נוספים.
- **קיום רוטציה בתפקידים מרכזיים בתחומי רכש וכספים.** החלפת בעל תפקיד מרכזי ורגיש מפחיתה את הסיכון כי תתרחש מעילה, מכיוון שהעובד מודע לכך שתקופת כהונתו בתפקיד קצובה בזמן ולאחר מכן ייכנס גורם אחר לנעליו.

בקרות שיכלו לגלות את המעילה

מעילה זו יכולה הייתה להתגלות על ידי קיומן של הבקרות הבאות:

- **בקרה תקופתית על שינויים בשדות רגישים של ספקים.** באמצעות בקרה זו החברה עוקבת אחר שדות רגישים ששונו, כדוגמת שם ספק, מספר חשבון בנק ועוד. כל שינוי בשדות אלה צריך להיות מגובה במסמך המאמת את הנתונים ששונו. לדוגמה, שינוי שם יהיה מגובה במסמך שעליו חתום הספק ובו השם החדש הרצוי, וכן מסמך של הבנק המאמת כי שם הספק תואם לשם חשבון הבנק.
- **ביצוע ניתוח נתונים במסדי הנתונים המרכזיים של החברה, במטרה לזהות מגמות ופעולות חריגות שבוצעו בתהליכים המבוצעים בחברה, כגון רכש, שכר וכספים.** חלק בלתי נפרד מהבקרות שמיישמות חברות הוא ביצוע ניתוח נתונים. לתחקור מסדי הנתונים של החברה יש ערך מוסף מפני שהוא מאפשר זיהוי פעולות חריגות (ככל שהיו כאלה), איתור דפוסי התנהגות, איתור חריגים שלא ניתן היה לזהות מביצוע סקרים ובקרות, ואיתור כשלים בבקרות הקיימות.
- **מבחני מהימנות לעובדים בתפקידים רגישים בתדירות שתיקבע מראש.** תפקידים בתחום הרכש והכספים מהווים משרות רגישות לאור מעורבותם בהוצאות כספי החברה. מומלץ, כי בעלי תפקידים הנוגעים באופן ישיר ועקיף לכספי החברה, יחויבו בביצוע מבחן מהימנות אחת לתקופה (בדרך כלל אחת לשלוש שנים). יש לציין, כי בקרה זו היא בנוסף על הבקרה המונעת, מפני שהידיעה של העובדים כי הם עתידים לעבור מבחן מהימנות משמשת כגורם הרתעתי.
- **חיוב עובדים בתפקידים רגישים בחברה לצאת לחופשה רציפה בת שבוע לפחות, במסגרתה תיחסם לעובד הגישה לתיבת המייל ולמערכות השונות בחברה.** במקרים שבהם עובד אחראי על ביצוע אותן פעולות מדי יום, עולה האפשרות כי הוא יצליח להסתיר פעולות אסורות. בעת יציאת העובד לחופשה רציפה, עובד אחר נכנס לנעליו ואחראי לבצע את אותן פעולות שמבצע העובד המקורי בכל יום. אם יהיו פעולות המבוצעות באופן תדיר ומוסתרות בכוונת תחילה, סביר להניח כי העובד המחליף יגלה זאת.

סיכום

קיים מגוון רחב של בקרות שניתן לשלב ולהטמיע הן כחלק ממערך הבקרה הרוחבי והן באזורים נקודתיים בתהליכי הרכש, כפונקציה של מאפייני הפעילות וגורמי הסיכון המבוססים על מיפוי תהליכים ייעודי, או כחלק מסקר מעילות והונאות שמומלץ לבצע אחת לתקופה. בקרות אלו אינן מחליפות את הצורך בתחקור מסדי נתונים לאיתור אנומליות, המהווה כיום כלי מרכזי באיתור חריגים.

ניתוח אירועי מעילה מעלה שברוב המקרים לא נדרש תחכום בביצוע המעילה, ומערך בקרה לקוי הוא שמאפשר את המעילה.

סוף הונאה
במחשבה תחילה

מאת

רו"ח ירון סעדי | ביקורת חקירתית, חטיבת הביקורת הפנימית, בנק הפועלים

רו"ח אסף חייק - לרנר | ביקורת חקירתית, חטיבת הביקורת הפנימית, בנק הפועלים

מהי הונאה?

להבדיל ממעילה (Embezzelment) המבוצעת לרוב על ידי גורם פנימי בארגון (עובד, מנהל, בעל מניות וכדומה), הונאה (Fraud) היא פעולת מרמה והטעיה המבוצעת על ידי גורם חיצוני לארגון (לקוח, ספק, נאמן, האקרים, גורמים עבריינים וכדומה), מתוך מטרה לקבל נכסים/כספים/זכויות במרמה תוך שימוש במצג שווא. ייתכנו גם מקרים שבהם נרקמת קנוניה בין גורם חיצוני לארגון לגורם פנימי בו כדי לבצע פשע כלכלי נגד הארגון.

לאורך שנים מתנהלת במערכת הפיננסית בישראל בכלל, ובמערכת הבנקאות בישראל בפרט, מלחמה סיזיפית נגד הונאות וניסיונות הונאה של גורמים חיצוניים. זוהי מלחמה המתנהלת ב"עצימות נמוכה" ומאחורי הקלעים.

מאמר זה מתמקד בעיקר בהונאות פיננסיות באשראי פרטי.

לכאורה, ברוב המקרים נזקי ההונאות ברמת המקרה הבודד אינם גבוהים ואין בהם כדי לאיים על יציבותם של המוסדות הפיננסיים, אך לכך יש לציין מספר סייגים:

- ראשית, ניסיון העבר מלמד כי בוצעו הונאות/ניסיונות הונאה בהיקפים גבוהים, במקרי קיצון עד כדי איום על יציבותו הפיננסית של הארגון שנפגע מכך. לדוגמה, בשנת 2005 בוצע ניסיון הונאת סייבר בהיקף של כ-220 מיליון ליש"ט על ידי כנופיית האקרים בינלאומית נגד השלוחה הלונדונית של בנק סומיטומו היפני.
  בשנת 2016 קבוצת האקרים הצליחה לפרוץ את מערכות המחשב של הבנק המרכזי של בנגלדש, ולהעביר 81 מיליון דולר מחשבונות בבנק הפדרלי של ניו יורק לחשבונות בתי קזינו בפיליפינים.
- חלק מהמוסדות הפיננסיים מגדירים את תיאבון הסיכון שלהם להונאות (ולמעילות) כ"תיאבון סיכון אפס", כלומר מצהירים הצהרה ערכית כי הם מוכנים לבצע את כל הצעדים הנדרשים כדי לצמצם למינימום האפשרי את היקף נזקי ההונאות בארגון.
- פרסום מידע לציבור בגין הונאות שכוונו נגד מוסדות פיננסיים, חושף את המוסדות לנזקי מוניטין, העלולים לעלות בהיקפם על הנזק הישיר שנגרם למוסדות אלו כתוצאה מההונאה.

בהקשר זה יצוין כי ניכר שבשנים האחרונות הרגולטורים (בנק ישראל, הממונה על שוק ההון, ביטוח וחיסכון) מקדישים תשומת לב פיקוחית גבוהה יותר לניהול סיכוני הונאות ומעילות בבנקים ובמוסדות פיננסיים.

המציאות העצובה היא שכפי שאנשים נורמטיביים יוצאים מדי בוקר להרוויח ביושר את מטה לחמם, ישנם אנשים/גורמים שהם "בעלי מקצוע" בתחום ההונאות. הם משקיעים את מיטב זמנם, מרצם, משאביהם ומוחם הקודח והיצירתי בניסיונות הונאה נגד בנקים ומוסדות פיננסיים. לצערנו, לא אחת הם מקדימים את המערכת הפיננסית בצעד אחד לפחות.

ממחקרים שנערכו בשנים האחרונות על ידי חברת PWC בנושא פשיעה כלכלית, עולה כי בתקופות של חוסר וודאות עסקית ומשברים כלכליים קיימת עלייה בפוטנציאל התממשותן של הונאות ומעילות. זאת, בעיקר כתוצאה מהסטת תשומת הלב הארגונית להתמודדות עם המשבר, אשר עלולה לגרום להיווצרות פרצות במנגנוני הבקרה הקיימים ובהזדמנויות לביצוע הונאות.

על פי סקר שנערך על ידי PWC לשנת 2017, 49% מהמשיבים דיווחו כי הארגון שלהם נפל קורבן למעילה או לפשיעה כלכלית. זו עלייה ניכרת בהשוואה לסקר משנת 2016 שבו 36% מהמשיבים דיווחו כי נפלו קורבן לפשיעה כלכלית. בסקר של 2017 ציינו שליש מהמשיבים כי הפשע הכלכלי החמור ביותר בארגון שלהם גרם להפסד ישיר של 50-100 אלף דולר (למקרה בודד).

לאילו הונאות חשופים הבנקים ומוסדות פיננסיים?

המוסדות הפיננסיים, ובראשם הבנקים, חשופים להונאות מסוגים שונים. להלן דוגמאות:

- הונאות סייבר/הונאות בתקשורת על סוגיהן השונים (פריצה למאגרי המידע וגניבת פרטי תעודות זהות/מספרי חשבונות/כרטיסי אשראי וכדומה, התחזויות/גניבת פרטי זיהוי לצורך העברת/משיכת כספים לזכות צד ג' שאינו מורשה, לרבות הונאות באמצעות אתר הארגון ובאמצעות מכשירים לשירות עצמי).
- הונאות אשראי שונות (אשראי קמעונאי, אשראי עסקי, הונאות בתחום סחר החוץ).
- התכחשויות לקוחות לביצוע פעולות בחשבונותיהם (משיכות מזומנים, העברות על סמך הוראה בדוא"ל/פקס, קבלת אשראי וכדומה).
- התחזות וגניבת זהות (באמצעות מסמכים מזויפים) לצורך קבלת כספים במרמה מהתאגיד הבנקאי.
- הונאות בכרטיסי אשראי.
- זיופי שיקים.
- הונאות לקוחות בכל הקשור לפעילותם בחדרי מסחר.
- הונאות המבוצעות על ידי ספקים/נותני שירותים בכל הקשור לתחום הרכש/לוגיסטיקה.
- הונאות ביטוח.

מלבד נזקי הונאות העלולים להתממש לנזק ישיר כלפי הבנקים, קיימים מקרים שבהם הבנקים ומוסדות פיננסיים חשופים לתביעות משפטיות או לתשלום שיפוי נזקי הונאות שבוצעו כלפי לקוחות הבנקים או על ידי לקוחות כלפי צד ג'.

בהקשר זה בולטות הונאות מסוג "הונאת פונזי" (המוכרת גם בשם הונאת "פירמידה"). בהונאה מסוג זה מובטחת למשקיעים תשואה גבוהה על כסף תוך פרק זמן קצר, בעוד בפועל הרווחים המחולקים למשקיעים הראשונים ממומנים מכספי המשקיעים שהצטרפו מאוחר יותר, עד לקריסת הפירמידה.

אין צורך להכביר במילים על ההונאה שביצע ברנרד מיידוף - הונאה בהיקף של כ-50 מיליארד דולר שבעקבותיה נגרם נזק בסכום של כ-1.7 מיליארד דולר ל- JPMorgan - הבנק שבו ניהל ברנרד מיידוף את חשבונותיו (סכום הנזק משקף את הסכם הפשרה שהושג כפיצוי לנפגעי התרמית).

אגב, בחלק מפסיקות בתי המשפט בישראל בשנים האחרונות, נקבע כי

מוסדות פיננסיים חבים חובת זהירות מוגברת (חובת נקיטת אמצעי זהירות סבירים למניעת הסיכון) לא רק ישירות כלפי לקוחותיהם אלא גם כלפי צד שלישי.

זאת בתנאי שהמוסד הפיננסי יכול היה לצפות כי צד שלישי יינזק.

הונאות אשראי קמעונאי

ההתקדמות הטכנולוגית שחוותה האנושות בעשורים האחרונים לא פסחה גם על המערכת הפיננסית. לפיכך "עלה קרנן" של הונאות הסייבר בתקשורת, שמטבע הדברים חושפות את המערכת הפיננסית לנזקים בהיקפים גבוהים.

עם זאת, בחרתי להתמקד במאמרי זה בהונאות אשראי קמעונאי (הניתן ללקוחות פרטיים), השייכות להונאות המוגדרות כבסיסיות יותר - "הונאות פיזיות", הנוגעות לליבת העיסוק של המערכת הבנקאית. לרוב, ברמת המקרה הבודד הונאות אלו מתבצעות בסכומים נמוכים יחסית, אולם ברמת האפקט המצטבר ניתן להניח שנזקי הונאות האשראי הקמעונאי המצטברים במערכת הפיננסית בישראל עלולים להסתכם בעשרות מיליוני ש"ח בשנה.

מאפיינים - הונאות אשראי בתחום הקמעונאי הן הונאות שעיקרן קבלת אשראי על סמך מצג שווא של כושר ההחזר של הלקוח, המתבסס על שימוש במסמכים מזויפים. בחלק מהמקרים גורמים עברייניים עושים שימוש באנשי קש, ומציידים אותם במסמכים מזויפים כדי לקבל אשראי. קיימת גם חשיפה לחבירת גורמים עברייניים לגורמי פנים במערכת הפיננסית לצורך ביצוע ההונאה. הונאת האשראי מתאפיינת גם בפרק הזמן הקצר החולף בין מועד ביצוע האשראי לבין מועד גילוי כשל פירעון האשראי.

להלן המאפיינים העיקריים של הונאות אשראי קמעונאי:

- שימוש במסמכים מזויפים/מצגי שווא לצורך הוכחת כושר החזר/יכולת פירעון של הלווה (דוחות כספיים, תדפיסי חשבון, תלושי שכר, חוזי שכירות, אישורי העסקה במקומות עבודה, תשלום משכורות פיקטיביות לחשבון הלווה וכדומה).
- הצהרה כוזבת לגבי מטרת/ייעוד האשראי או לגבי מקורות פירעון האשראי, או לגבי נאותות/אמיתות הבטחונות שהועמדו לאשראי.
- היעדר זיקה ישירה (גאוגרפית, עסקית או אחרת) של הלווה (הלקוח) לסניף או ליחידה שבהם בוצע האשראי.
- הפניית לקוחות לפתיחת חשבונות ולקבלת אשראי על ידי גורמים בעלי היסטוריית אשראי בעייתית, לעיתים תוך מעורבות של גורמי פשיעה (לעיתים האשראי מיועד לגורם המפנה). בחלק מהמקרים אף נעשה שימוש באנשי קש על ידי גורמים עברייניים לצורך פתיחת חשבונות חדשים שבהם יבוצע אשראי.
- זיוף חתימת לקוחות על גבי מסמכי אשראי.
- משיכת מלוא/רוב תמורת האשראי במזומן בסמוך למועד ביצוע האשראי, כדי להקשות על נתיב ביקורת לשימוש בתמורת האשראי.
- העברת תשלומי משכורת "פיקטיבית" לחשבון הלווה (לעיתים באופן חד-פעמי) כבסיס לקבלת אשראי, ומאוחר יותר החזרת "המשכורת" לגורם המעביר.

- פירעון האשראי על ידי צד ג' (שאינו הלווה).
- נקיטת פעולות מרמה לשחרור בטחונות/שיעבודים בטרם פירעון האשראי.

בחלק מהמקרים עושים גורמים שונים ניסיון לאתר נקודות תורפה במערכת הפיננסית (איתור עובדים חסרי ניסיון ו/או שימוש בטכניקות של הנדסה חברתית) כדי להקל על ביצוע הונאת האשראי. במקרי קיצון אף קיימת חשיפה לביצוע קנוניה של גורם חיצוני עם עובד מוסד פיננסי לצורך ביצוע הונאת האשראי.

צעדים למניעת/צמצום הונאות אשראי

ניתן לנקוט צעדים שונים לצורך מניעה או צמצום נזקי הונאות האשראי, הן ברמת הטיפול במקרה הבודד ביחידת הקצה והן ברמה המערכתית בארגון:

בשלב מימוש האשראי

- נקיטת משנה זהירות במתן אשראי ללקוחות חדשים, בפרט ללקוחות שאין להם זיקה ישירה (גאוגרפית, עסקית או אחרת) לסניף או ליחידה שבהם בוצע האשראי.
- ביצוע בדיקת נאותות (על סמך מידע ציבורי הקיים ברשת האינטרנט) בגין לקוחות, מעל לסכום אשראי מינימלי שייקבע.
- נקיטת משנה זהירות בקשר עם לקוחות שהופנו על ידי גורמים שבמהלך בדיקת נאותות זוהה מידע שלילי אודותם.
- אימות נתוני מקום העבודה/תדפיסי חשבון של לקוח חדש המקבל אשראי.
- גילוי ערנות לגבי אנומליות במסמכים המוגשים במסגרת בקשת האשראי (חשד למסמכים מזויפים).
- (במקרים הרלוונטים) תשומת לב לצד ג' המתלווה ללקוח בעת תהליך פתיחת החשבון/קבלת האשראי, ובפרט תשומת לב לצד ג' המגלה דומיננטיות בעת ביצוע שיחת ליבון הצרכים עם הלקוח, מבקש האשראי. בהתאם נדרשת תשומת לב ומשנה זהירות, כאשר במקרים אלה הלקוח מגלה פסיביות ו"אינו שולט" בפרטי בקשת האשראי שהגיש.
- (במקרים הרלוונטיים) הקפדה על תיעוד פרטי הגורם שהפנה את הלקוח לקבלת אשראי.

לאחר ביצוע האשראי

- תשומת לב לאשראי שתמורתו/רוב תמורתו נמשכת במזומן בסמוך למועד הביצוע.
- תשומת לב לפירעון אשראי על ידי צד ג'.

בקרות מערכתיות

- **על הארגון לוודא כי סיווג ומדידת הונאות האשראי מתבצעים באופן נאות.** המטרה היא למנוע מצב של הערכת חסר של היקף נזקי הונאות האשראי של הארגון (לנוכח האפשרות שחלק מנזקי הונאות האשראי מסווגים בטעות ככשלי אשראי). מטבע הדברים, לנתוני היקף נזקי הונאות האשראי יש השלכה על היקף המשאבים שמוכן הארגון להקצות לצורך ניטור ומניעת/צמצום הונאות מסוג זה.
- **ניהול מידע אודות שיטות וגורמים בקשר עם ביצוע הונאות אשראי.** קיימת חשיבות לצבירת המידע בגין אירועי הונאות אשראי ולתיעודו במאגר מידע ייעודי: סכומים, חשבונות שבהם בוצעו הונאות, פרטי מבצעי ההונאות, גורמים מפנים, סוג ההונאה, מאפייני ההונאה ועוד.

  קיימת חשיבות לתיעוד כל המידע לגבי הונאות שהתגלו בארגון במאגר אחד מרכזי (בכפוף למגבלות המשפטיות הרלוונטיות לניהול מאגרי מידע).

  ניהול מאגר מידע יאפשר איתור וזיהוי של טכניקות ודרכי הונאות אשראי, מגמות חריגות בנושא זה, וגורמים חיצוניים בולטים בתחום הונאות האשראי, ויסייע בהטמעת דרכי פעולה מתאימות לצמצום או למניעת הישנות המקרים.
- **פיתוח כלי בקרה בגין הונאות אשראי (בכפוף לשיקולי עלות-תועלת) שיציפו התראות/"אורות אדומים".** לדוגמה: מתן אשראי ללקוחות שהופנו על ידי גורמים שעל פי מידע ציבורי היו מעורבים בביצוע הונאות, חשבונות שבהם בוצע אשראי (שאינם שייכים לאותה קבוצת סיכון) והוזרמו אליהם פרטים מינהליים זהים (כתובות, כתובות דוא"ל, מספרי טלפון וכדומה), פירעונות אשראי בחשבונות לקוחות על ידי צד ג', וכדומה.

הכשרות לעובדים בנושא טכניקות הונאה וזיהוי חשד או סמאנים לניסיון מסמכים, לדוגמה:

- **תדפיסי חשבון בנק** עם יתרות לא נכונות, סכומי פעולות עגולים בלבד, שדות מידע חסרים, סוגי/תיאור פעולה שאינם אחידים/עקביים.
- **תלושי שכר** עם סכומי משכורת (נטו) עגולים החוזרים על עצמם כל חודש, יתרת מחלה/חופשה מאופסת, גובה משכורת (נטו) שאינו תואם את סכום זיכוי המשכורת בתדפיס החשבון, מספר תעודת זהות שאינו זהה למספר תעודת הזהות של הלקוח, היעדר מספר חשבון בנק לזיכוי בתלוש השכר.
- **תעודת זהות** שתאריך הנפקתה שונה מתאריך ההנפקה על פי נתוני מרשם האוכלוסין או שמודפסת בסוגי גופן שונים, או שהגיל על פי תעודת הזהות אינו תואם את גילו של מבקש האשראי.
- **דוחות כספיים או מסמכים אחרים** החתומים לכאורה בחותמת רו"ח ללא פרטים, או על גבי נייר לבן ללא כותרת, או מסירת דוחות כספיים זהים עבור מספר חברות/תאגידים שונים וכדומה.

2018
ALL STAR
CONFERENCE

OCT. 22 - 24, 2018
Aria Resort & Casino
LAS VEGAS, NV
THE BEST AND MORE

ביצוע הפקות לקחים מאירועי הונאות

חשוב להפיק לקחים מאירועי הונאה בולטים שהתגלו, על מנת לנסות ולאתר חשיפות הקיימות לבנק/מוסד פיננסי ולמנוע הישנות מקרים דומים בעתיד.

סיכום

בסיכומו של דבר, על דרך המליצה ניתן לומר ש"סוף הונאות במחשבה תחילה" - ניהול לא נאות של סיכוני ההונאה עלול במקרי קיצון לחשוף מוסדות פיננסיים עד כדי איום על יציבותם. אמנם לא ניתן לחסום הרמטית את ניסיונות ההונאה של גורמים עברייניים, אך היערכות נכונה ברמה המערכתית וברמת יחידות הקצה, ניטור יזום של ניסיונות הונאה על בסיס המידע והניסיון שנצבר בארגון, בד בבד עם הטמעת כללי הזהירות בכל רובדי הארגון והפקות לקחים אפקטיביות בעת הצורך, עשויים בהחלט לצמצם למינימום את נזקי ההונאה לארגון.

מי האחראי???

רשלנות תורמת של הארגון למעילה

מאת
עופר אלקלעי | רו"ח, אלקלעי מונרוב
סרגי גאורגייב | רו"ח , אלקלעי מונרוב

מעילה. לא אחת מתברר שכיסיו של המועל ריקים (זו הרי היתה המוטיבציה למעילה...),
לא נערך ביטוח לכיסוי מעילות (הוא יקר...) והארגון פונה למעגל השלישי - הבנק או רואה החשבון.

במאמר זה נדון ברשלנות תורמת של הארגון למעילה:
האם גם לארגון שבו בוצעה המעילה קיימת אחריות לאי גילוי המעילה?
מה היקף האחריות כאשר מתברר שהארגון לא נקט אמצעים סבירים למניעתה?

הסוגיה נידונה בפס"ד אל שרד בע"מ נ' יובנק בע"מ מתאריך 10.02.2014.

סיפור המעילה

מעיון בכתב התביעה עולה כי חברות אל שרד ופולימוד הן חברות הפועלות כחלק מקבוצת חברות העוסקת בתחום האופנה - קבוצה בעלת מחזור שנתי של מאות מיליוני שקלים. אל שרד, פולימוד וחברות נוספות בקבוצה, פעלו במסגרת "איחוד עוסקים" לצורכי דיווח מע"מ. לפולימוד לא היו אמצעי תשלום או חשבון בנק, ולכן לצורך ביצוע תשלומים לספקי החברה נעשה שימוש בחשבון הבנק של אל שרד שנוהל ביובנק - שקיבל לידיו את טופס דוגמאות החתימה של מורשי החתימה בחברות. יש לציין כי שירותי המטה, לרבות שירותי הנהלת חשבונות וביצוע התשלומים, ניתנו לכל החברות בקבוצה ובהן פולימוד, על ידי מחלקת הכספים של הקבוצה שמנתה בין 11 ל-20 עובדים.

> "החברות שלא נקטו אמצעי בקרה בסיסיים הן הנושאות באחריות למעילה ויש לייחס להן אשם תורם בשיעור של 100%"

לפי כתב התביעה, מנהלת החשבונות (גברת סגל) של חברת פולימוד הייתה אחראית לביצוע תשלומים לספקים ולרישום פקודות יומן מתאימות בספרי החברה, ואף קיבלה לידיה את ההמחאות של אל שרד בצורה שוטפת וללא בקרה על השימוש שנעשה בהן. בשנת 2006, לאחר שפוטרה עקב אי שביעות רצון מעסיקיה, גילתה עובדת שהחליפה אותה בתפקידה כי המחאה בסך 10,572 ש"ח שנפרעה מחשבון אל שרד, לא הופיעה בספרי הנהלת החשבונות של פולימוד ונרשמה לפקודת גורם שאינו קשור לחברות. בבדיקה נוספת התגלו 345 המחאות בסך כולל של כ-5 מיליון ש"ח שנפרעו מחשבונה של אל שרד על ידי גורמים שאינם קשורים לקבוצת החברות, ונמצא כי החתימות שעל גבי ההמחאות - זויפו.

התברר כי המעילה הוסתרה באמצעות רישום כוזב של פקודות יומן בכרטיסי הנהלת החשבונות של החברות, בעיקר כנגד כרטיס "מע"מ תשומות" וכנגד כרטיסים נוספים של הוצאות, קניות והשקעות.

לאחר גילוי המעילה חתמה גברת סגל על הודאה והתחייבות לשיפוי החברות, אך מאחר שלא הצליחה להחזיר את כספי המעילה, הגישה קבוצת החברות תביעה כנגד יובנק בדרישה לקבל פיצוי.

בתביעה נטען כי על פי תנאי החוזה שבין הבנק ללקוחותיו, הבנק מתחייב לבצע פעולות בחשבון רק בכפוף להוראת מורשי החתימה. לטענת התובעים, אילו נהג הבנק בזהירות הראויה כמתחייב בחוזה, היה מגלה בנקל את הזיוף לאור ההבדלים שבין דוגמאות החתימה שנמסרו לו לבין החתימות המזויפות שהופיעו על ההמחאות, וכך היה עוצר את המעילה ומצמצם את נזקיה.

להגנתו טען הבנק כי בדק את ההמחאות כמתחייב על פי רמת סבירות ראויה ולא הפר את חובותיו, וכי החברות שלא נקטו אמצעי בקרה בסיסיים הן הנושאות באחריות למעילה ויש לייחס להן אשם תורם בשיעור של 100 אחוזים.

שאלת האחריות – על מי?

כדי לקבוע את גבולות האשם והאשם התורם, דן בית המשפט בשאלות שלהלן:

1 האם קיים דמיון סביר בין הזיוף לדוגמת החתימה?

שאלה זו נועדה לקבוע את מידת אחריותו של הבנק לאיתור המעילה. אם קיים דמיון סביר בין הזיוף לדוגמת החתימה, הרי שלבנק אין יכולת למנוע את המעילה. משמעות הדבר היא שבמקרים של זיופים מתקדמים, בהם למשל נסרקות חתימות מורשים, טענות נגד הבנק יידחו על הסף.

2 האם בדיקת ההמחאות על ידי הבנק נעשתה באמצעים סבירים ובאופני פעולה סבירים?

כחלק מניהול הסיכונים, קבע הבנק כי המחאות ייבדקו רק מעל לסכום מסוים, ושממוצע הזמן לבדיקת המחאה אחת יעמוד על כ-30 שניות. כמו כן, החתימות של לקוחות משתנות עם הזמן, ואין לבנק אפשרות מעשית לפנות לכל הלקוחות על מנת לאמת את השינוי. בסופו של דבר הבנקים "קונים סיכון", ומעדיפים להסתכן בתביעה מאשר לשלם מיליוני שקלים על שעות עבודה של פקידים שיבדקו לעומק כל המחאה.

לאור זאת, בית המשפט קבע כי האמצעים שנקט הבנק לבדיקת ההמחאות הינם סבירים.

3 האם הבנק נקט אמצעי זהירות לצמצום ומניעת הנזק?

הדיון בשאלה זו נועד כדי לחלק את האחריות בין הצדדים. מחד, אמצעי הזהירות היחיד שבידי הבנק הוא בדיקת חתימות המורשים, אך מאידך מדובר באמצעי זהירות משמעותי ביותר, שכן איתור חתימה מזויפת או אפילו תשומת לב להיעדר דמיון סביר בין החתימה שעל גבי ההמחאה לדוגמת החתימה, היו מצמצמים את היקף המעילה ואולי אף מונעים אותה.

עם זאת, קיים מספר רב של אמצעי זהירות נוספים שעל החברה לנקוט, שמכלולם היה מצמצם את היקף המעילה ברמת ודאות גבוהה.

בחוות דעת שהגיש מומחה מטעם הבנק עלה כי החברות לא נקטו אמצעי זהירות שעשויים היו לצמצם את היקף המעילה.

- לא נערכה בדיקת רקע ואמינות לגברת סגל בטרם החלה לעבוד בתפקיד משמעותי ורגיש, אף שסבלה ממבנה אישיותי של מועלת סדרתית ועל אף עברה כמהמרת.
- החברות לא הקפידו על הפרדת תפקידים ואפשרו לגברת סגל הן לקבל המחאות באופן שוטף (וללא בקרה על השימוש שבוצע בהן) והן לרשום את פקודות היומן בספרי החברות.
- החברות לא פיקחו על הנפקת פנקסי ההמחאות.
- לא התבצע פיקוח על ספחי ההמחאות ששולמו לגורמים שונים.
- לא נערכה בדיקת רציפות להמחאות שהופקו לתשלום.
- ההמחאות שנמשכו מחשבון הבנק לא הוצלבו עם אסמכתאות מגבות לתשלום (למשל חשבוניות).
- **לא מונה מבקר פנימי לחברה ולא נערך סקר חשיפה למעילות.**
- לא נאכפה חובת היציאה לחופשה רציפה בת שבעה ימים לכל הפחות.
- לא בוצעו בקרות שוטפות ונקודתיות בנושאים נוספים, כגון בדיקת פקודות יומן חריגות, שימוש ב"דוחות חכמים" ועוד.
- לא הוטמעה מערכת מחשוב מתקדמת בעלת מערך הפרדת תפקידים מובנה, לא נעשה שימוש במדפסת ייעודית להדפסת המחאות על דף נייר חלק, ולמרות שבבעלות החברות הייתה מערכת להפקת המחאות ממוחשבות, גברת סגל הפיקה מאות המחאות ידניות שמטבען הן בעלות סיכון גבוה יותר למעילה.

עוד קבע המומחה, כי החברות שכאמור לא נקטו אמצעי זהירות מלבד ביקורת רו"ח והתאמות בנקים, ויכלו לגלות את המעילה בשלב מוקדם יותר אלמלא התעלמו מהדגלים האדומים שהיו לנגד עיניהם:

- זיוף מאות המחאות המהוות כ-33% מכלל ההמחאות שהופקו, כלומר כל המחאה שלישית הייתה מזויפת.
- רישום הוצאות בכרטסות הנהלת החשבונות ללא אסמכתאות מגבות.
- גידול חריג במע"מ התשומות, המשקף עליה של כ-22 מיליון ש"ח בהוצאות פולימוד - גידול זה אינו משקף את מחזור ההוצאות האמיתי של החברה.
- רישום פקודות יומן חריגות, ללא כל היגיון חשבונאי.

באי כוח התובעת טענו, כי האחריות נופלת בצורה מלאה על הבנק שכשל בבדיקת החתימות על ההמחאות, וכי מדובר במעילה מתוחכמת שלא ניתן היה לעלות עליה בנקל.

לאחר שמיעת טענות הצדדים, דרכי המעילה, הבקרות והכשלים שהתגלו, קבעה השופטת דניה מאיר קרת את המסקנה הבאה:

"מהדיון באמצעי הבקרה השונים - אלו שלא בוצעו בשל חוסר סבירות או חוסר רלוונטיות מזה ואלו שבוצעו אך נעקפו מזה, מצטיירת תמונה ברורה: המעילה הייתה מתוחכמת למדי ובקרות סבירות שהפעילה התובעת, נעקפו על ידי העובדת. העובדת ניצלה נקודות תורפה שהינן אינהרנטיות לאופייה החשבונאי של החברה.

עם זאת, אין ספק שלצד ניצול נקודות תורפה "לגיטימיות", הסך הגדול של בקרות שלא בוצעו, מוביל למסקנה כי החברה שגתה בניהול חשבונותיה.

מקובלת עלי גישתו של רו"ח אלקלעי, אשר חזרה על עצמה בגרסאות רבות הן בחוות דעתו והן בחקירתו, לפיה על אמצעי הבקרה הננקטים להתאים לנקודות התורפה בהתנהלותה של החברה והאחריות להתאמתם, כמו האחריות למניעת מעילות בכללותה - מוטלת על הנהלת החברה.

נוכח האמור, עולה המסקנה כי התנהלות החברה בפיקוח על העובדת ובפיקוח על השיקים שיצאו מחשבונה, לא הייתה סבירה וכי היא מקימה לה אשם תורם. העובדה כי מחשבונה נמשכו מאות שיקים במשך כשנתיים מצביעה על כך שלא יתכן שכל האשם יוטל לפתחו של הבנק."

סיכום

בסיכומו של דבר, קבעה השופטת כי לחברה אשם תורם בשיעור של 25 אחוזים מהנזק (המהווים כ - 1.2 מיליון ש"ח).

פסק הדין קבע כי האחריות הראשית למניעת המעילה בזיוף חתימות על המחאות רובצת על הבנק. עם זאת, אין להתעלם מקביעת השופטת כי על הארגון להתאים את הבקרות כך שיוכלו לאתר ולמנוע מעילה מתמשכת ובהיקף כספי גדול.

אין הארגון יכול להניח כי הבנק או רואה החשבון, גם אם התרשלו, יישאו בכל הנזק, כאשר בו-בזמן הוא לא פעל באופן סביר למניעת המעילה.

2 סדנאות לתחקור נתונים בתוכנת IDEA

יתקיימו בתאריכים

למתחילים 7,9.10.2018

למתקדמים 15,21.10.2018

במשרדי דלוייט, מגדל עזריאלי עגול, קומה 42 תל אביב

המפגשים יתקיימו בין השעות: 15:00 - 19:00

פרטים והרשמה: מזכירות IIA ישראל 03-5116617

כל סדנה מקנה 7.5 שעות CPE

סדנת כתיבה והשבחת דוחות ביקורת

נובמבר 2018

בהנחיית בעז ענר

פרטים והרשמה:
מזכירות IIA ישראל
03-5116617

ערב עיון

בנושא תשאול

יתקיים בתאריך 10/10/2018
במשרדי דלוייט 16:00-19:30

מרצה:
רונן ארצי

פרטים והרשמה:
מזכירות IIA ישראל
03-5116617

מקנה 3 שעות CPE

הערך הכספי של ביקורות לזיהוי טעויות

מאת
כריסטופר קלי

מתן מרב תשומת הלב לסיכונים של טעויות והונאות מהותיות הוא נושא שחוזר על עצמו במסגרת התקנים המקצועיים הבינלאומיים של לשכת המבקרים הפנימיים העולמית (IIA's International Professional Practices Framework, IPPF). לדוגמה, על פי תקן תכונות מס׳ 1220, חובה על מבקרים פנימיים להפעיל זהירות מקצועית ראויה ולהתחשב ב״הסתברות של טעויות משמעותיות, הונאה, או אי-ציות״.

במגזר הציבורי והפרטי, סביר להניח שטעויות במהלך העסקים הרגיל אינן נגרמות בכוונה תחילה. הונאה מוגדרת בתקנים כ״כל מעשה בלתי חוקי המאופיין על ידי תרמית, הסתרה או הפרת אמונים המבוצע בכוונת תחילה״. הדיכוטומיה בין טעות לא מכוונת לבין הונאה אינה תמיד ברורה.

נראה ששיטות ביקורת מסוימות מתאימות יותר לאיתור טעויות והונאות. שיטות הנסמכות על הצגת ההנהלה, או שלפיהן ניתן למבקר אישור שהבקרות אכן פעלו כמתוכנן - כגון ראיונות, רשימות תיוג להערכה עצמית, מבחני הדרכה בשטח, דגימת עסקאות, ובדיקת סבירות אנליטית - עשויות להיות חשופות להטיית אישור (הנובעת מאמונתו או מדעתו הקיימת של המבקר). אפשר שהמסקנות לא תהיינה שנויות במחלקות, אך הן עלולות לפגוע בשמה הטוב של הביקורת הפנימית כאשר בהמשך מתגלות טעויות מהותיות או הונאות.

אם לא התקיים עם המבוקר דיון מעמיק על פעולות מתקנות במהלך הישיבה המסכמת, ניתן לטשטש טעויות והונאות במידה רבה. מתוך ניסיון של שנים רבות עולה שלעיתים יישום המלצות מתמהמה או שההמלצות מיושמות באופן פחות נחרץ ממה שהמבקר הפנימי

"באמצעות זיהוי טעויות והונאות מהותיות, מבקרים יוכלו להמחיש את ההשפעה של בקרה כושלת בצורה טובה יותר"

התכוון. מכאן עולה שהטיית אישור בעבודת השטח, בשילוב עם פעולות מתקנות שלא נדונו מספיק ולא יושמו כהלכה, יכולות להסתיר טעויות מהותיות והונאה המתרחשות בתדירות גבוהה יותר מהמצופה. אחת הדרכים להקטין את הסיכון של מתן הבטחה מוטעית ולחזק את מעמדו של המבקר הפנימי בעיני חברי הדירקטוריון היא לחפש את הטעויות שהבקרות הפנימיות אמורות למנוע.

איתור טעויות

איתור טעויות מהותיות והונאה דורש העלאת השערות לגבי תרחישים אפשריים של מעילות והונאות. באופן אידיאלי, הדבר מתאפשר על ידי שילוב ניסיון רב-מגזרי בחשיבה יצירתית - החל מהתרחיש הגרוע ביותר שניתן לצפות לו - ובהמשך, תכנון ביקורת שטח בידיעה מוקדמת שהממצאים עשויים להיות שונים מהמשוער.

שיטות לאיתור טעויות כוללות:

- הצלבת מקורות מידע שבדרך כלל לא תואמים, כגון מטא-דאטה לטלפונים ניידים ונתוני הנכנסים למבנה.
- שימוש בכריית מידע.
- שימוש בחוק Benford להדגשת תנועות יוצאות דופן.
- בירור תכולת דאר אלקטרוני.
- הקשבה לעובדים שעשויים להסכים לחשוף מידע על בקרות שנעקפו.

קל יותר לשכנע את ההנהלה לגבי השפעת הבקרה החלשה כאשר מאתרים טעות ממשית בעלת השפעה ברת-כימות.

כך יש לביקורת הפנימית טיעון חזק לשיפור תהליכים, והתנגדות ההנהלה לכך תיחלש כאשר טעות אחת או טעויות רבות מובאות לדיון בפגישת הסיכום.

לביקורת הפנימית יש יתרון הנובע מכך שלרוב עומדים לרשותה כלים לכריית מידע, רשת של קשרים מהימנים בארגון שיכולים להוות מקור מידע בעל ערך רב, וכן תמונה רחבה של תהליכים מקצה-לקצה בזמן שעובדים רבים מוגבלים לפרספקטיבה הצרה של מחלקתם. המבקר הפנימי, על ידי מינוף היתרונות הללו, יכול לזהות את מה שלא ברור לאחרים.

העלאת השערות על תרחישים של טעויות והונאה בתכנון הביקורות שלנו עבור ארגונים שונים, אפשרה לצוות הביקורת הפנימית לחזק את המוניטין שלו לגבי הממצאים. צעד זה זכה לתגובות מהירות מצד ההנהלה, להשבת סכומי כסף משמעותיים, ובמקרים רבים אף הוביל להחלפת עובדים.

מקרה מס. 1

על ידי זיהוי חריגות מתקרות הפקדה, איתרה הביקורת הפנימית 75 מיליון לירות סטרלינג בפיקדונות של חברה בריטית לשירותי תשתית. הסכום יועד למקסום ריבית בנקאית, אך חרג בהרבה מתקרת ההפקדות שאושרה על ידי מועצת המנהלים באותם מוסדות פיננסיים.

ההנהלה העדיפה את האינטרס שלה בכך שהיא מקסמה בונוסים אישיים מבוססי הכנסות, תוך עקיפת "התיאבון לסיכון" של מועצת המנהלים. האינטרס האישי של ההנהלות נצפה לעיתים קרובות כהעדפה שהתגלתה בביקורות לזיהוי טעויות.

מקרה מס. 2

מבקרים פנימיים חשפו מיליון דולר אוסטרלי בדיווחי מחלות וחופשות כוזבים שלא דווחו כנדרש על ידי עובדים בחברת תחבורה אוסטרלית. ההונאה התגלתה תוך העלאת השערה שהונאות מסוג זה אפשריות, וכן איתור טעויות על ידי הצלבת נתוני שכר כנגד שימוש בטלפון סלולרי, שימוש ברכב, נתונים ונתוני הנכנסים למבנה החברה.

תחילה ניסתה ההנהלה לטעון שהביקורת הפנימית הפרה את תקנות הפרטיות בכך שהיא חקרה את מקום הימצאותם של העובדים. אך המבקר הפנימי הראשי הוכיח שעל פי תקנות הפרטיות, שימוש במטא-דאטה של הארגון עצמו מותר לצורך בירור הימצאותם של עובדים בשעות העבודה.

מסקנת הביקורת הייתה שלא זו בלבד שתרבות העובדים הייתה לקויה ויש צורך לתקנה, אלא שגם תרבות הפיקוח לקויה,

דבר שהוביל לשינויים רבים בצוות ההנהלה. למהלך זה הייתה השפעה חיובית על פריון העבודה, על התחייבויות לחופשות במאזן, וכן על עלויות של שעות נוספות שנגרמו כתוצאה ישירה מדיווחים כוזבים של העובדים לגבי היעדרותם במשך שנים רבות.

מקרה מס. 3

על ידי העלאת תרחישים לטעויות לפני ביצוע ביקורות שטח ובמהלכה, זיהתה הביקורת הפנימית 8 מיליון ליש"ט בחיובי יתר שגויים מצד קבלני תחזוקה של חברת הנדסה בריטית. נמצאו כ-50 מקרים נפרדים של טעויות והונאה, מוסתרים בתביעות לסכומי כסף חד-פעמיים, וחתומים על ידי מחלקת ניהול לקוחות לאחר בדיקות נאותות לקויות טרם אישורם לתשלום.

חרף חתימות רבות של מנהלי החברה (עד למנכ"ל), כל מנהל הניח שהמנהל מתחתיו ביצע את הבדיקות המפורטות לחיובי הקבלן. ברגע שחיובי היתר כומתו על ידי הביקורת הפנימית, הושבו מרבית הסכומים ללא צורך בעורכי דין. התפתחות מפתיעה שנבעה מאותה ביקורת התרחשה כאשר המנכ"ל של אותה חברה הנדסית קודם לתפקיד בכיר יותר בחברה גדולה, והוא גייס את המבקר הפנימי הראשי לשורותיה.

מקרה מס. 4

בבדיקת ספרי החשבונות של נכסים בלתי מנוהלים, אותרה יתרת חוב בסך 4 מיליון לירות סטרלינג של חברה בת בריטית של חברה אמריקאית.

החוב חמק מעיניה של מחלקת בקרת אשראי משום שהוא נוצר על ידי לקוחות חריגים מחוץ למהלך העסקים הרגיל, ולכן עקף את דוח הגבייה השגרתי. התברר ש-50% מהחוב היה ניתן לגבייה, מה שהוביל לגבייה של כ-2 מיליון לירות סטרלינג ולמאזן "נקי" יותר.

מקרה מס. 5

מחלקת התשלומים לספקים לא הצליחה לאתר 2 מיליון דולר אוסטרלי בתשלומים כפולים לספקים בקרב לקוחות קמעונאיים, תחבורה, משרדי ממשלה וחברות הנדסה. על אף שניתן היה לגלות את הכפילות במערכת לניהול חשבונות ספקים עוד לפני התשלום, התראות המערכת בוטלו או שהממונים המקומיים התעלמו מהן. הביקורת הפנימית עשתה שימוש במידע שברשותה כדי לבצע בדיקות עצמאיות לכריית מידע, שהתמקדו במיוחד בגילוי כפילויות.

להפתעתנו, נמצאו עשרות כאלה. התשלומים המיותרים הושבו להנהלה על ידי הספקים והוחזרה הבקרה לאיתור ומניעת תשלומים כפולים.

מקרה מס. 6

המבקרים הפנימיים גילו פיקדון של 60 מיליון דולר אוסטרלי בחשבון בנק יחיד של חברת תחבורה אוסטרלית. הפיקדון נשא ריבית אפסית, בשל חוסר התייחסות מצד ההנהלה להשגת תשואה על כספי החברה. מועצת המנהלים הסכימה שמוטב היה להשקיע את הכסף במספר מוסדות וברמת סיכון נמוכה, על מנת להשיג תשואה שנתית של 900,000 דולר אוסטרלי לפחות.

בשני המקרים הללו,

היעדר דוח ההשקעות הסתיר ממועצת המנהלים כיצד נותבו הכספים, והתוצאה הייתה שכסף רב הוחזק במקומות הלא נכונים.

מקרה מס. 7

במקרה שמשקף טעויות והונאה מהותיות, זיהתה הביקורת הפנימית נהלים לשימוש ברכב שנוסחו באופן גרוע ולא יושמו באופן תקני בשתי חברות נפרדות. בנוסף, חברות ליסינג חיצוניות הוסיפו חיובים לא נחוצים לטובתן.

כתוצאה מכך נעשה שימוש במרמה ברכב החברה למטרות שונות שאינן עסקיות. חברות האם לא היו מודעות לביטול רישיונות נהיגה בשל היעדר הצהרות של נהגים, וחלה עלייה בשיעורי תאונות רכב, שגרמה לעלייה בפרמיות הביטוח. חברות הליסינג הטילו קנסות לא מוצדקים בעת סיום השכירויות. על אף שלא הצליחו להשיב את מלוא העלויות הקודמות, החברות נמנעו מלשלם מיליון דולר אוסטרלי בעלויות שנתיות עתידיות על ידי שיפור הנהלים והבקרות כתוצאה מהביקורת.

מקרה מס. 8

לעיתים מתגלות טעויות והונאות באמצעות רשת הקשרים של הביקורת. אזהרה מעורפלת אך קריטית מטעם אחד העובדים גילתה שמנהל הכספים העביר מידע קנייני ממועצת המנהלים לחברה למערכות מידע. חברה זו הגישה הצעות מחיר לחוזים בעשרות מיליוני דולרים, כאשר מנהל הכספים היה דירקטור ובעל מניות באותה חברת IT.

הביקורת הפנימית אימתה את מעורבות מינהל הכספים בחברה השנייה עם הרגולטור של ניירות ערך, ובהמשך ניצלה את זכויות הגישה המוקנות לה מתוקף כתב האמנה שלה לצורך בדיקת הדואר האלקטרוני ורישומי הטלפון הסלולרי של מנהל הכספים כדי לאמת את העברת המידע הקנייני. החברה סיימה את עבודתו של אותו מנהל כספים, הסדירה את נוהל ניגוד האינטרסים, השיבה חלק מהעלויות ההיסטוריות ושמה קץ להוצאות עתידיות לא נחוצות הנאמדות במיליוני דולרים.

המקרים הנ"ל ממחישים מגוון כשלים במדיניות, בניהול סיכונים, בשיטות ובניסוח החוזים. את כל אלה ניתן לגלות באמצעות איתור טעויות והונאות מהותיות במהלך תכנון וביצוע ביקורות.

ראיות חותכות

בקרב ארגונים חל שיפור ניכר בהערכת המוניטין של המבקר הפנימי, כאשר ראיות לטעויות מהותיות שקשה לחלוק עליהן הובאו לדיון במועצת המנהלים. לעיתים קרובות, טרם הפצת דוח הביקורת, חלו שיפורים בבקרות, הושבו הוצאות, נמנעו עלויות פוטנציאליות, ובמקרים החמורים ביותר - העובדים העבריינים סיימו את תפקידם.

מועצות מנהלים מעדיפות שזיהוי הטעויות ייעשה בשלב מוקדם על ידי המבקר הפנימי,מאשר לאחר האירוע על ידי בקרות חיצונית, רגולטורים, או פרסום באמצעי התקשורת. גם אם לא יימצאו כשלים במתודולוגיה לזיהוי טעויות, הרי זו כשלעצמה מהווה סוג של הבטחה (אם כי לא מוחלטת) באשר ליעילות הבקרות.

המאמר תורגם מגיליון דצמבר 2017 של כתב העת:
INTERNAL AUDITOR | The dollar value of error seeking audits by Christopher Kelly

תרגום | עו"ד שלומית איתן
CIA, מנהלת מחלקה ביקורת ניהולית, חברת החשמל לישראל

הונאת השותף

מאת

ג'ימס קרול | BDO USA - CRMA CPA/CFF, CFE

תיאור המקרה

בשותפות לקבלנות בנייה בשם "Building Co The (TBC)", עם הכנסות שנתיות של 8 מיליון דולר, יש שני שותפים. מייק בילינגס, המנהל והבעלים, ייסד את TBC וזמן קצר אחר כך הכניס את סטיב גריי כשותף שווה, המחזיק כמוהו בשיעור של 50% בשותפות. בילינגיס הכיר את גריי מעבודתם המשותפת בעבר וצירף אותו לחברה בשל הרקע החזק שלו בתחום המכירות. על אף העובדה שאף אחד מהשותפים לא חתם על הסכמי ניהול משותף, בילינגס מילא את תפקיד נשיא החברה ומנהל רשום, וגריי החזיק בתפקיד סגן הנשיא במסמכי המיסוי של החברה.

כל אחד מהשותפים משך משכורת, ובהתאם להסכם לא פורמלי בין השותפים, כל אחד מהם היה רשאי להעביר כספים מ-TBC לטובת הוצאות אישיות. בסוף השנה, השותף שמשך פחות כספים לטובת הוצאות אישיות, היה יכול למשוך כסף במזומן להשוואת ההוצאות בין השותפים. בעוד שבילינגס התמקד בהרחבת העסק ובניהול פרויקטים ופיתח אסטרטגיה עסקית, אחריותו של גריי כללה מעקב עלויות והכנסות, ניהול יומיומי של המשרד, שיווק, פרסום וניהול הספרים. על אף שלגריי לא הייתה השכלה בתחום החשבונאות או בתחומים אחרים הקשורים בפיננסים, בילינגס סמך עליו באופן מוחלט.

בשלב מסוים החל בילינגס לחשוש מהפעילות של שותפו העסקי. גריי לא הכין מסמכים פיננסיים פנימיים שהתבקש להכין חודשים קודם לכן, לרבות הצהרה על הוצאות שותף לשנה הנוכחית ודוחות כספיים תקופתיים. לנוכח חששותיו ערך בילינגס סקירה ראשונית, ניתח תנועות תשלומים נבחרות וזיהה עסקאות מרובות שבוצעו על ידי גריי לטובת עסקים אחרים שלו, כולל עסקה אחת בהיקף של 300,000 דולר.

לאחר הניתוח הראשוני פנה בילנגס ליועץ וחוקר בתחום החשבונאות לביצוע חקירה, במטרה לבחון האם זכויות הצדדים בשותפות נשמרו. החוקר שלף וניתח מידע מהמחשבים ומהטלפונים העסקיים של גריי, ובנוסף ניתח את כל המסמכים הפיננסיים הרלוונטיים, כולל הוצאות בכרטיס אשראי פרטי ועסקי של גריי.

נושאי החקירה

החקירה התמקדה בנושאים הבאים:

1. שליפת כל הנתונים החשבונאיים והפיננסיים מתוכנת החשבונאות בתקופה שנבדקה.
2. קבלת כל החוזים הרלוונטיים ותיעוד תומך.
3. מינוף הידע שיש לבילינגס על עסקיו האחרים של גריי, היכרותו עם ספקי TBC שסביר להניח שגריי נעזר בהם בשיפוץ ביתו, והבנתו של בילינגס את חיובי כרטיס האשראי שאינם מיוחסים לעסקי TBC.
4. עריכת ראיונות לעובדי TBC להבנת הבקרות הפנימיות והתמקדות בנושאים ספציפיים הרלוונטיים לחקירה.
5. תקשורת שוטפת עם ההנהלה על מנת להבטיח את עדכונם של בעלי העניין בנושא ובהתפתחותו.

מסקנות החקירה

החקירה העלתה שבתקופה של שלוש שנים, גריי מעל בסכום של מעל 450,000 דולר, שהופנו לטובת אורח החיים הראוותני שניהל, שכלל הימורים, נסיעות יקרות לחו"ל וביקורים תדירים במועדוני חשפנות.

מתוך בושה, גריי השתמש בכרטיסי האשראי של החברה כדי לשלם על ההוצאות האישיות האלו, ללא ידיעתו של בילינגס. החיובים בכרטיס אשראי זה כללו חיובים עבור הוצאותיו של גריי ושל עובדי TBC אחרים על הימורים, מסעדות ומועדני חשפנות. גריי רשם את העסקאות הללו כ"לקוחות/ בידור לקוח" בפנקסי חשבונות ראשיים שונים. לאחר מכן לא כלל את העסקאות הללו בדוחות בעלי המניות שערך.

ניצול של אמון ופיקוח מוגבל – שותפים עסקיים משתמשים בחברה כבנק למימון הוצאות אישיות

בנוסף, גריי הגה תוכנית על מנת לשלם מכספי החברה את החיובים בכרטיס האשראי האישי שלו: הוא יגיש ויאשר את דוח ההוצאות שלו (בחתימתו) ואז ינפיק לעצמו המחאה מ-TBC שגם עליה הוא חתם או שינפיק תשלום ישיר מ-TBC לחברת

כרטיסי האשראי שלו. זיהוי ההוצאות הלא-מנוכות שלא נוצלו, חייבו לבצע פעולות חשבונאיות טכניות נוספות והתמודדות עם נושאי מס שדרשו פתרון.

גריי גם נתן הלוואת גישור לאחד מעובדי TBC לרכישת בית. בשיחה שהתקיימה עם העובד שקיבל את ההלוואה התברר שגריי חייב אותו בריבית בסך 15,000 דולר ל-30 ימי ההלוואה. את הריבית גריי השאיר לעצמו, ובנוסף החזיר ל-TBC 250,000 דולר מתוך הלוואה של 300,000 דולר.

כאשר נבחנו הבקרות הפנימיות והמידע הפיננסי הרלוונטי ב-TBC, החוקר מצא שגריי השתלט באופן מלא על כל התהליך והמידע הפיננסי של TBC, והיה מסוגל לעשות מניפולציות על המידע הפיננסי שניתן לבילינגס ולבעלי העניין. גריי שינה את דוחות הרווח של הפרויקטים על מנת שלא לכלול "הוצאות לא עסקיות". הוצאות אלה נרשמו בחשבונות הוצאות כלליות ושוייכו לפרויקטים רק לפני סיום הפרויקט או לאחר השלמתו. דוחות הפרויקטים מראים בבירור הוצאות נוספות שנוספו לדוח סמוך לסיום הפרויקט או לאחריו.

גריי גם תמרן את ספר החשבונות הראשי של TBC באמצעות אפיון לא נכון או סילוף תיאור ההוצאות האישיות, כגון שיפור מקום מגוריו הפרטי ורכישת מכשירים חדשים. לצד הרישום כהוצאות כלליות צורף תיעוד תומך אמין וכשר, ובמקרים מסיימים לא צורף תיעוד התומך בתקפות העסקה.

בנוסף, הוא הסווה את ההוצאות הלא עסקיות באמצעות רישומם כחיובים בדוחות הרווח של הפרויקט או תשלום פרטי לספקים בהוצאות קבלני משנה. במקרים רבים הוא רשם את החיוב השקרי בקטגוריית הוצאות קבלני משנה, מכיוון שזאת הייתה ההוצאה הגבוהה ביותר בפרויקט, ובילינגס לא היה בודק הוצאה זאת לפרטיה.

מלבד היעדר הפרדת תפקידים בניהול הפיננסי, החוקר גם גילה שגריי חתם על רוב ההמחאות ופיקח על מנהל החשבונות החיצוני, במשרה חלקית, שרשם את העסקאות בהתאם להנחיות של גריי. גריי גם שלט בממשק עם יועץ מס, וסיפק לו את כל המידע הפיננסי הרלוונטי, ללא ידיעתו של בילינגס. למרבה הצער, בשל תשתית IT לקויה של TBC, השרת שלה לא מגבה את מערכת החשבונאות, ולכן כל המידע החשבונאי שלפני 2012 אבד.

בסופו של דבר, בילינגס רכש את חלקו של גריי בעסק במחיר שמתחשב בכספי המעילה, אך בחר שלא להגיש תביעה כדי למנוע יחסי ציבור שליליים ואובדן לקוחות פוטנציאלים. TBC, בילינגס וגריי החזירו כספי מיסים עבור שלוש השנים האחרונות וכן נדרשו לשלם מיסים נוספים וקנסות.

הלקח שנלמד

- ניתן למזער את הסיכונים שמוצגים בסוג זה של שותפות במגוון דרכים, לרבות עריכת בקרות של השותף שלא עוסק בפיננסים, סקירת דוחות בנקאיים, קבלת דוחות כספיים באופן אוטומטי ממערכת החשבונאות, וסקירה חיצונית של רו"ח מעת לעת.
- הסכמים המסדירים את ההסכמות העסקיות בין השותפים, חייבים לכלול פרטים על אחריותו של כל צד. פרטים אלה יוכלו לשמש את המבקרים בעריכת ביקורת ולתיאום ציפיות.
- מבקרים פנימיים צריכים לעבוד עם יועצים משפטיים לבחינת עמידה בחוקים ועל מנת להבטיח שההשלכות החוקיות של החקירה נלקחות בחשבון.
- בעסקים קטנים ובינוניים, הביקורת הפנימית צריכה להבטיח שבעלי העניין נוטלים חלק בסביבת הבקרה הפנימית. ניתן להשיג זאת באמצעות בקרת ניטור, כגון סקירה בודדת ונפרדת של דוחות כספיים ועירובם של כל הגורמים הרלוונטיים בממשקים עם גורמים חיצוניים הקשורים בפיננסים.
- תמיד צריכה להיות בדיקה של גורם נוסף לגבי המחאות, על מנת לוודא את אמינות התיעוד התומך, מקבל התשלום והסכום.

המאמר תורגם מגיליון אוקטובר 2017 של כתב העת:
INTERNAL AUDITOR | Fraud Findings by JAMES CARROLL

תרגום | עו"ד שלומית איתן
CIA, מנהלת מחלקה ביקורת ניהולית, חברת החשמל לישראל

מערכת ניהול למניעת שוחד (ISO 37001) ועבודת הביקורת הפנימית

מאת

ד"ר דביר פלג | CISO, CRO - סוקר תאימות לדרישות ISO

התקינה הוולונטרית בנושא מניעת שוחד, עונה לצורך המתעורר בעקבות עליית המודעות הציבורית לבעיית השוחד, השינויים בחוקי הכסף המזומן, המלחמה בהון השחור והעיסוק התקשורתי בנושאים אלה.
זאת עד שרשויות החוק ידביקו את הפער ויקבעו רגולציה עולמית המותאמת למצב.

רקע:

ארגון התקינה הבינלאומי (ISO - International Organization for Standardization) הוא גוף בינלאומי הקובע תקנים. תקני ניהול - ISO - הם כללים לאסדרה כלכלית בארגונים. בארגון חברים גופי תקינה לאומיים מרחבי העולם והוא כותב תקנים ניהוליים, תעשייתיים ומסחריים בינלאומיים. יישום התקנים הוא וולונטרי, אלא אם כן החליטה הממשלה להחילם כתקני חובה. לדוגמה, על פי החלטת ממשלה, תקן ניהול אבטחת המידע ISO 27001 הוא תקן חובה בכל משרדי הממשלה.

ועידת היסוד של הארגון, שהתכנסה תחת הסיסמה learning between equals, חיפשה שם שייצג את השוויון ומצאה אותו במילה היוונית isos, שמשמעותה היא בלנס - שוויון. בפועל, תיאוריית ראשי התיבות אינה נכונה, שכן שם הארגון הוא International Organization for Standardization ולא International Standards Organization.

תקנים אלה מהווים "רגולציה וולונטרית" (ללא כפייה חוקית), המתבצעת על ידי שימוש בכלים רכים כגון הדרכה, הגברת המודעות ושיתוף הפעולה. בכך דומים תקני הניהול לפעילות הביקורת הפנימית, שגם מטרתה היא לשפר את פעילות הארגון ואת יכולתו להשיג את מטרותיו.

בשנה האחרונה נוסף תקן ניהול חדש: "מערכת ניהול למניעת שוחד", שמספרו: ת"י ISO 37001. הצורך במערכת ניהול וולונטרית נוצר בעקבות חוסר אחידות בחוקי השוחד בעולם, וכן בגלל קושי ברגולציה ובאכיפה עולמית.

"מערכת ניהול למניעת שוחד" היא מערכת כללים ותהליכים שהארגון מתחייב לבצע וכן להיסקר על ביצועם על ידי גוף חיצוני אחת לשנה.

למה כדאי לארגון ליישם מערכת ניהול למניעת שוחד?

בארגונים רבים הנחשפים לקיומה של התקינה בנושא מערכת ניהול למניעת שוחד (ת"י ISO 37001), נשאלת שאלת הנחיצות. על מנת לענות לשאלה זו נקביל את מניעת השוחד למניעת הטרדה מינית: עד שהפכה לחוק, מניעת הטרדה מינית הייתה רגולציה וולונטרית שארגון התחייב לה. ריבוי האירועים, העיסוק הארגוני והעיסוק התקשורתי בנושא הביאו לחקיקת חוקים מפורשים ולרגולציה מחייבת, ויותר מכך - הביאו לשינוי הנורמה הציבורית והפרטית.

כך גם בתחום מניעת השוחד. העיסוק התקשורתי והציבורי העולה, החלת נורמות מוסר ונורמות שיפוט ציבוריות על המגזר הפרטי בארץ ובעולם (אישום בישראל בגין שוחד שניתן בחו"ל), כמו גם חוקי הכסף המזומן המשתנים והשפעת המלחמה בהון השחור ובפשע ב"מרשתת האפלה" (Darknet), כל אלה מחייבים שימוש ברגולציה וולונטרית עד שרשויות החוק יקבעו רגולציה עולמית המותאמת למצב.

בנוסף, חוק החברות מחייב את הדירקטוריון בחובת זהירות. ניתן לראות את מערכת הניהול למניעת שוחד (ת"י ISO 37001) כחלק מחובת הזהירות של הדירקטורים לארגון ושל הארגון לדירקטורים.

מה צריכה לכלול מערכת ניהול למניעת שוחד?

1. דרישה לכתיבת והטמעת מדיניות המעלה את נושא השוחד, קבלה ומתן של מתנות, טובות הנאה ותרומות, מהרמה הארגונית הלא פורמלית אל רמת ההנהלה.

נדגיש שלגבי סחיטה מובהר בפרשנות לתקן כי סחיטה היא "תשלום כאשר כסף מוצא בכוח מצוות העובדים באמצעות איומים על הבריאות, הבטיחות או החירות שלו או של אחרים". מכיוון שמערכת החוק בחוק העונשין אינה רואה בתשלום עקב סחיטה מעשה פלילי, לגבי סחיטה - הארגון יכול לקבוע מדיניות המתירה ביצוע תשלום, הגדרת דרכי הפעולה, תיעוד האירוע, התשלום ודיווח לממונה על מניעת שוחד בארגון.

2. דרישה לזיהוי כלל החוקים, הצווים והתקנות בנושא שוחד בכל אתרי פעילות החברה בארץ ובעולם, זיהוי כל בעלי הממשק העסקי, ונושאים פנימיים וחיצוניים המשפיעים על מניעת השוחד בחברה, לדוגמה:

- גודל, מבנה והיקף האצלת הסמכויות של מערכת קבלת ההחלטות בארגון.
- מיקום הפעילות של הארגון והסקטור שבו הוא פועל.
- מהות ומורכבות הפעילויות של הארגון.
- המודל העסקי של הארגון.
- הארגונים שתחת שליטתו והארגונים ששולטים עליו.
- בעלי ממשק עסקי.
- היקף ואופי יחסי הגומלין עם גורמים רשמיים.
- דרישות על פי דין, דרישות חוזיות והנחיות גופי מקצוע והנחיות ישימות שהארגון אימץ.

3. מינוי ממונה על מניעת השוחד בארגון - בעל תפקיד עם קשר ישיר לדירקטוריון ולהנהלה הבכירה, האחראי על מניעת שוחד בארגון. בסמכותו להעריך את סיכוני השוחד בכל המחלקות והפרויקטים, לקבוע נהלים, ובעיקר להגביר ולאכוף את חובת הדיווח, לתחקר אירועים ולהעלות להנהלה "דגלים אדומים".

מספר העובדים במערך הציות (מערך האכיפה של מניעת השוחד) יהיה בהתאם לגודל הארגון ולרמת הסיכונים לשוחד שאליהם הארגון חשוף. בארגון קטן יכול להתמנות לתפקיד זה אדם הנושא תפקיד שגרתי בארגון, אך יש לוודא שתפקידו אינו בסיכון גבוה לקבלת שוחד (מנהל רכש למשל). גורם הציות חייב להיות בעל כישורים (השכלה, הדרכה וניסיון), מעמד בארגון (דעתו נשמעת ומיושמת) וסמכות (הרשאת האכיפה מספקת), עצמאי וחסר תלות.

4. הגדרת אחריות וסמכות לכל בעל תפקיד בנושא מניעת השוחד.

5. קביעת שיטה מתועדת לזיהוי סיכוני שוחד וניגוד עניינים: במסגרת השיטה ייערכו ניתוחים, הערכות ודירוג של הסיכונים שזוהו. וכן יוערכו האמצעים לבקרה ומניעת שוחד ויותאמו לארגון. אם יעלו סיכונים פוטנציאליים (דגלים אדומים), תבוצע בדיקת נאותות.

הסיכון ייבחן גם בנוגע להעסקתם של עובדים ועובדי כוח אדם זמניים. לגבי האחרונים ניתן להפחית את הסיכון הן על ידי החלת הבקרות שנקבעו לגבי עובדי הארגון גם על עובדים אלו, או על ידי חיוב מעסיקם להפעיל את הבקרות.

קביעת השיטה לזיהוי סיכוני שוחד מסייעת גם בקביעת גבולות ברורים בארגון בנושאים "אפורים" לכאורה כמו קבלת תשורות (לדוגמה: קבלת שוקולד או בקבוק יין מלקוח למחלקת תשלומי ספקים - לא תמיד לאנשי המחלקה יש כלים להעריך את שווי התשורה, ולעיתים לאורך השנים נוצרים גם ניגודי עניינים כאשר הספק הופך לחבר אישי המזמין ומוזמן לאירועים אישיים, והשוקולד הופך לכאורה לתשורה פרסונלית ולא תשורה בגין תפקיד), אירוח, תרומות, מוצרים ממותגים וכו'.

כאשר עולה חשד לסיכון שוחד, כלומר לא זוהתה פעילות שוחד אולם הנסיבות או האירועים עלולים ליצור מראית עין או פוטנציאל לכך, תבוצע **בדיקת נאותות**.

בדיקת נאותות היא למעשה המשכו של תהליך בחינת הסיכונים לגבי פרויקטים, עסקאות, פעילויות ארגוניות, שותפים עסקיים ועובדים שלגביהם נמצא כי הם מהווים סיכון בינוני או גבוה לשוחד. את בדיקת הנאותות יש לערוך אחת לתקופה בהמשך לסקר סיכוני השוחד, והיא מהווה בקרה ממוקדת על מניעת שוחד בתחומים הנבדקים.

בקרה בנושא ניגוד עניינים ניתן לבצע על ידי מתן שאלונים לבעלי תפקידים בתחומים שהארגון זיהה כרגישים, כגון רכש, ניהול פרויקטים וכו', ובעקבות הבדיקה יש לקבוע "דגלים אדומים" - נורמות ארגוניות או אירועים המעלים חשש לניגוד עניינים או מצבים חריגים שמצריכים בדיקה בתחום מניעת השוחד.

לדוגמה, מנהל פרויקטים שעבד אצל לקוח ועבר לעבוד בחברה - יש לבחון האם המעבר התבצע בעקבות צורך או בעקבות מערכת יחסים שהיטיבה עם החברה תחת ניהולו של המנהל, או יחסי משפחה או שכנות בין מנהל הרכש למי מהספקים.

6. אימוץ בקרות פיננסיות ושאינן פיננסיות: בקרות פיננסיות הן התהליכים המיושמים על ידי הארגון לניהול נכון וראוי של העסקאות הכספיות, וכן לתיעוד מדויק, מלא, ומהיר ככל האפשר שלהן. בקרות שאינן פיננסיות הן תהליכים המיושמים על ידי הארגון כדי לוודא כי היבטים לא כספיים של הפעילויות מנוהלים באופן נכון וראוי.

7. הדרכת כל עובדי החברה, הספקים וקבלני המשנה, משלב הקבלה לעבודה ואחת לתקופה במשך העסקת העובד בחברה.

8. עריכת מבדקים פנימיים תקופתיים הבוחנים את אפקטיביות המערכת ואת אופן ניהולה. מטרת המבדק היא לספק ביטחון סביר לדירקטוריון ולהנהלה הבכירה כי מערכת מניעת השוחד שהוקמה פועלת באופן אפקטיבי, וכן לייצר הרתעה ניהולית.

9. ביצוע סקרי הנהלה שבהם נבחנת עדכניות המדיניות והנהלים, נבחנים כלל האירועים שדווחו וכן הפעולות שבוצעו בעקבותיהם, מאושרר סקר הערכת סיכוני השוחד, וכן נקבעים יעדים ותוכניות עבודה בתחום.

מה טיב הקשר בין תקני הניהול לעבודת הביקורת הפנימית?

האם מערכת ניהול למניעת השוחד תורמת לעבודת הביקורת? ראוי לזכור כי כל מערכת ניהול הנסקרת בקביעות של אחת לשנה על ידי גוף חיצוני בלתי תלוי מחזקת את עבודת המבקר. המבקר מוגבל לעיתים על ידי תוכניות עבודה ושיקולים ארגוניים של קובעי התוכנית, בזמן שגוף חיצוני חופשי ממגבלות אלו ויכול לחזק את גבולות הארגון ולהגביר את כושרו התחרותי והשגת מטרותיו.

חוזקו ויתרונו של מבדק חיצוני עולה ככל שהפתיחות ורמת שיתוף הפעולה בין הסוקר לעורכי המבדק הפנימי (שיכולים להיות המבקרים הפנימיים) של הארגון עולה גם היא.

עורך מבדק פנימי יכול לכוון את הסוקר למקומות שבהם הוא מזהה בעיה, אולם כוחו הפוליטי, הארגוני, עלול להיות חלש יותר, וסוקר חיצוני יכול לתמוך בשיפור תהליכי הארגון על ידי שיקוף תהליכי הארגון בעזרת עורך המבדקים הפנימי.

לסיכום, ניתן לראות קווים מקבילים בין עבודת יחידת הביקורת לתקני הניהול - ולכן למרות השוני ניתן לראות בתקני הניהול בכלל ובמערכת ניהול למניעת שוחד בפרט כלי משלים ותומך בעבודת הביקורת.

פורום "שולחן עגול"
למבקרים פנימיים ראשיים

כמה פעמים הייתה לך הזדמנות להיות חבר בפורום שיכול להשפיע על פעילות הביקורת הפנימית ועל עתיד הביקורת בכלל?

המפגש הבא של הפורום יתקיים ביום **ראשון ה- 16 בספטמבר 2018**
במשרדי שיכון ובינוי רחוב הירדן 1א קריית שדה התעופה

להרשמה למפגש הקרוב יש לפנות ל**ליאת רסיין פרי** מנהלת לשכת נשיא האגוד
טלפון: 03-5116617 | office@theiia.org.il

* החברות בפורום מוגבלת למבקרים פנימיים ראשיים בלבד.
בפורום כ- 60 חברים המשמשים כמבקרים פנימיים ראשיים בארגונים המובילים בישראל.

קורס לימודי תעודה
ביקורת פנימית

מטרת הקורס הינה להקנות למשתתפים - ידע תיאורטי ומעשי במקצוע הביקורת הפנימית, הכולל בין השאר חוק ותקנים מקצועיים, ביקורת בסביבה ממוחשבת, טכניקות וכלי ניהול הדרושים לצורך ביצוע ביקורת פנימית.

IIA ישראל

המפגשים יתקיימו בימים א׳ ו-ה׳
11-12/2018

בין השעות
19:00 - 16:00

פרטים והרשמה: מזכירות IIA ישראל, ליאת רסין פרי
03-5116617

מקנה 36 שעות CPE

סיור מקצועי במוזיאון
"הרצליינבלום"

בנק דיסקונט | בהובלת מבקר הבנק מר ניר אבל

יתקיים בתאריך 8.10.18 בשעות 09:00 – 12:00
פרטים והרשמה: מזכירות IIA ישראל 03-5116617

קץ הביקורת? על הבלוקצ'יין ועתיד הביקורת

מאת

ד"ר יוסי נטוביץ | רו"ח, מנכ"ל טיוב יועצי מערכות

האם הטכנולוגיה עומדת לייתר את הצורך בביקורת והבטחה (Assurance)? האם פריצת דרך טכנולוגית תאפשר ניהול ממוחשב אוטונומי של ספרי חשבונות החסינים מפני שיבושים והונאות ובלתי חדירים לפריצה? מייקל קייסי ופול ויגנה מה"וול-סטריט ג'ורנל" פורשים בהרחבה בספרם החדש "מכונת האמת" (The Truth Machine) חזון שלפיו סביר מאוד כי טכנולוגיית הבלוקצ'יין (Blockchain) תספק לשאלות אלו תשובה חיובית. לנוכח ההשפעה הצפויה של טכנולוגיה זו על עתיד הביקורת והעולם העסקי בכלל, חשוב לבחון אותה ולעקוב אחריה.

האם אכן יש למבקרים, חיצוניים ופנימיים, סיבה לדאגה? לדעתי ייתכן שטמונה להם כאן דווקא הזדמנות.

אמון בעולם העסקים

קשה להפריז בחשיבות האמון בין הצדדים בעולם העסקים המודרני. המשקיעים לא ישקיעו במיזם שאין להם אמון במנהליו, והסוחרים לא ישלחו סחורה לקונה אם אין להם אמון שהם יקבלו תמורה. במרוצת השנים השכילה האנושות לפתח ולשכלל מערכת אמון גלובלית המאפשרת לשני צדדים לבצע ביניהם עסקאות על אף שאינם מכירים זה את זה באופן אישי. רק באמצעות מערכת האמון שפותחה, המשק הבינלאומי יכול לשנע סחורות ושירותים בין מדינות ויבשות על פני תבל. המערכת מונעת בעזרת רשת של "סוכני אמון" ומתווכים הנאמנים על הצדדים - בנקאים, עורכי דין, מבקרים, שמאים ועוד, ומשמשים "שמן סיכה" בתהליך ביצוע העסקאות. כלי מרכזי שמערכת האמון משתמשת בו הוא ספר החשבונות (Ledger) המשקף את המציאות העסקית של העסק.

אלא שמערכת האמון הזו סובלת ממספר פגמים. העיקריים שבהם: עלויות התיווך הגבוהות בין העסקאות (הסוכנים, הבנקאים והאחרים גוזרים עבור חלקם בעסקה קופונים שמנים), וכן מקרים חוזרים ונשנים של כשלים, כגון ספרי חשבונות שאינם מציגים "אמת" ו/או סוכני אמון הפועלים באופן מוטה.

ספר חשבונות מבוזר

טכנולוגית הבלוקצ'יין פותחה כתשתית רשת מחשבים לביצוע עסקאות בביטקוין - המטבע הקריפטוגרפי שאינו נתון לשליטה או בקרה מרכזית מצד גורם כלשהו. הבלוקצ'יין היא התוכנה שמנהלת בצורה אוטומטית את הרישום של עסקאות המסחר בביטקוין ואת השליטה והבקרה עליהן באופן מבוזר במחשבים שונים ברשת.

חשוב להפריד בדיון בין הביטקוין (ומטבעות דיגיטליים אחרים), שהשימוש בו כמטבע לגיטימי שנוי במחלוקת ועתידו עדיין לא ברור, לבין הבלוקצ'יין, שהוא כאמור תוכנת רישום ובקרת העסקאות שניתן לעשות בה שימושים רבים מגוונים.

מאז נוצר הביטקוין בשנת 2009 על ידי קבוצת מפתחים עצמאית בראשותו של "סאטושי-נקמוטו" (שם בדוי, זהותו האמיתית לא ברורה), המסחר על בסיס תוכנת הבלוקצ'יין משגשג והיא מעולם לא נפרצה.

זו ההוכחה לכך שניתן ליצור את האמון הדרוש לקיום קשרים עסקיים בין צדדים באמצעות תוכנה חכמה, וכי דרך זו יכולה להיות תחליף חסכוני יותר ובטוח יותר לעומת השימוש בסוכני האמון המסורתיים.

כיצד פועל הבלוקצ'יין?

בלוקצ'יין הוא ספר חשבונות דיגיטלי המשותף לחברי רשת מבוזרת של מחשבים עצמאיים. הספר מעודכן ומנוהל באופן שמאפשר לכל אחד לוודא את שלמות ותקינות הרשומות בעזרת אלגוריתמים שמשולבים בתוכנה.

הפוטנציאל של הבלוקצ'יין מעודד השקעות עצומות ברחבי העולם.

כל מחשב מנהל באופן עצמאי עותק של הספר שאמור להיות זהה לחלוטין לעותקים במחשבים האחרים, כך שגם אם האקרים יצליחו לחדור לאחד המחשבים ולגרום לשיבוש בנתוני הספר או שאחד מחברי הרשת ירצה "לבשל" הונאה, הרי שהשינוי בעותק יתגלה אוטומטית על ידי אלגוריתם להבטחת קונצנזוס בין העותקים ויתוקן.

תנועת יומן חדשה שנוצרת (למשל עסקת העברה של סכום בביטקוין בין חברי הרשת) נחתמת בצורה דיגיטלית, כך שכולם יכולים לאמת את מקורה. משתתפי המסחר רשומים ומוצגים במערכת תחת שם קוד, אך זהותם נשמרת בה בסודיות.

הספר מורכב מבלוקים של תנועות יומן, ה"משורשרים" ביניהם לפי סדר כרונולוגי בקשר לוגי: תנועות חדשות מאוגדות כל מספר דקות לבלוק נתונים דיגיטלי חדש, המשורשר מתמטית לבלוק הקודם ונענל באמצעות חתימה. כל שינוי שייערך בנתוני הבלוק ייצור אי התאמה מתמטית עם הבלוק הקודם ויתגלה. כך מבטיח השרשור בין הבלוקים שהתנועות אינן ניתנות למניפולציה.

עבודת שרשור בלוק חדש דורשת משאבי מחשוב יקרים ולכן היא מזכה את המחשב המבצע בתגמול כספי במטבע דיגיטלי. בשפת הבלוקצ'יין עבודה זו מכונה בשם "כרייה" (Mining). ברשת קיימים "כורים" רבים המתחרים ביניהם. הכורה שנבחר מתוכם לבצע את העבודה הוא המחשב שיפתור ראשון "חידה" קריפטוגרפית הקשורה לבלוק זה. לאחר השרשור, עותק מהבלוק החדש משודר לכל מחשבי הרשת.

אחת היכולות המעניינות של הספר המבוזר היא "חוזים חכמים" - הוראות ממוחשבות לביצוע עסקאות באופן אוטומטי, בהתקיים תנאים מוסכמים מראש. לדוגמה, חוזה שדומה במקצת לכתב אופציות: אם בתאריך עתידי מחיר נייר ערך יותר גבוה מסכום מוסכם, אז צד אחד משלם לצד השני את ההפרש.

טכנולוגיה בהתפתחות

כדי לפרוץ לעולם מן המעבדות וה"פיילוטים" שבהם היא נחקרת כיום ולהפוך לטכנולוגיה נפוצה בשימוש רחב, בלוקצ'יין עדיין צריכה להתגבר על מספר בעיות מהותיות ובהן:

1. מגבלת היקפי התנועות הניתנות לעיבוד.
2. תצרוכת חשמל יקרה וכוח עיבוד עצום הנדרש לפעולת הכרייה.

3. גם אם הבלוקצ'יין עצמו מאובטח כראוי, התוכנות לניהול כספים במערכות בסביבת הבלוקצ'יין, כגון החוזים החכמים, עדיין נכתבות על ידי תוכניתנים שונים ובאופן לא סדור ולכן סובלות מחולשות אבטחה. בעבר כבר התרחשו אירועים של פריצות וגניבות כספים באמצעותן.

עם זאת, הפוטנציאל של הבלוקצ'יין מעודד השקעות עצומות ברחבי העולם, וכעת מפותחות גרסאות חדשות ומתקדמות המתמודדות עם הבעיות הקיימות במטרה למצוא להן פתרון.

"אינטרנט של ערך"

מודל ספר החשבונות המבוזר, המשמש בעיקר כתשתית לניהול מסחר במטבעות קריפטוגרפיים כדוגמת ביטקוין ואתרים ללא צורך בפיקוח מרכזי, מלהיב את דמיונם של יזמים ומשקיעים רבים שרואים בו פוטנציאל לפתרונות יישומיים נוספים לניהול חדשני, חסכני ומבוזר של נכסים דיגיטליים. מספר דוגמאות מני רבות:

- ניהול זכויות בעלות על נכסים: מקרקעין (טאבו), מכוניות וכו'.
- ניהול מאגרי תכנים דיגיטליים תוך שמירה על זכויות היוצרים - כגון מוזיקה, צילומים וספרים.
- ניהול מעקב תנועות בשרשרת האספקה.
- ניהול רשתות מאובטחות של מקורות אספקה של אנרגיה סולרית.
- ניהול רשתות תקשורת מאובטחות של התקני אינטרנט של דברים (IoT).

עם זאת, יש להסתייג ולומר כי ניסיון העבר מלמד שהתלהבות יתר הנוצרת סביב טכנולוגיה חדשנית בהתהוות, נוטה לראות בה פתרון קסם כמעט לכל בעיה ולא תמיד על בסיס מוצדק.

הבלוקצ'יין מעורר עניין רב במיוחד במגזר הפיננסי, שם הוא נתפס כטכנולוגיה "משבשת" שעלולה לשמש תשתית לביצוע עסקאות פיננסיות בין עסקים ללא צורך בבנקים.

כדי להקדים תרופה למכה התאגדו בנקים בפרויקטים משותפים להקמת פלטפורמות בלוקצ'יין, כדוגמת R3-Corda, שיישלטו במידת מה על ידם.

עתיד הביקורת ושירותי ההבטחה

לפי קייסי וויגנה, גם ענף הביקורת נערך ל"כוננות ספיגה": "ארבע הפירמות הגדולות נוקטות גישה של אם אינך יכול לנצח אותם, הצטרף אליהם." נכון לאמצע שנת 2017, דלויט בלבד מעסיקה 250 עובדים במעבדות ספר החשבונות המבוזר שלה. וגם שלוש האחרות עוסקות בכך באגרסיביות. אמנם מדובר בחלק קטן מכל כוח העבודה שלהם, אולם המחקר והפיתוח הייעודי בנושא מלמדים על הרצינות שבה הפירמות מתייחסות לטכנולוגיה זו. אם ספרי חשבונות מבוזרים וחסינים לשינוי הופכים למציאות, הרי שחטיבות הביקורת והחשבונאות ייהפכו בסופו של דבר למיותרות ותהיה לכך השפעת ענק על התעסוקה. חטיבות הביקורת וההבטחה (assurance) בפירמות מעסיקות כ-300 אלף עובדים ותורמות כ-40% מהכנסותיהן הגלובליות הכוללות, המגיעות לכ-127 מיליארד דולר.

לפירמות אלה ברור כי החשבונאות, כפי שאנו מכירים אותה, המבוצעת באופן רבעוני ובמסגרתה קבוצות סוקרות מדגם של עסקאות בעבר על מנת להעריך את התקינות של אירועי העבר - תתייתר. "ארבע הפירמות הגדולות הן רק קצה הקרחון - לא רק הן בסיכון, אלא למעשה כל המבקרים, כולל המבקרים הפנימיים של הארגונים", אומרים קייסי וויגנה.

האומנם "קץ הביקורת"?

האם באמת ספר החשבונות המבוזר המאובטח מעמיד בסימן שאלה את הצורך במבקרים ורואי חשבון אנושיים? לדעתי טענות אלה מבוססות על תפיסה פשטנית ומצמצמת של הביקורת כפעולת אימות טכנית של שלמות רישומים והתאמות בין ספרי הצדדים לעסקאות.

בדיווח כספי, "אמון" מתייחס להיבטים מורכבים יותר, כגון קיומו של נכס פיזי - האם הנכס הרשום אכן קיים? הבלוקצ'יין אפקטיבי באימות קיום נכסים דיגיטליים כגון ביטקוין, אולם לקיום נכסים פיזיים עדיין יידרש אימות חיצוני. דוגמה נוספת: נאותות הערך הכספי והחתך - בהתייחס למכלול התנאים של העסקות הרלוונטיות ותחזית השלמתן בעתיד (לדוגמה, האם החוב ישולם? האם הסחורה תסופק?) - האם ערך הנכס הרשום אכן תואם לערך הכלכלי/חשבונאי של הנכס? כמו כן, האם הסיווג ואופן ההצגה הוא הוגן? אין צורך לומר כי טכנולוגית הבלוקצ'יין לא תסייע באימות הערך.

יותר מזה, בהתייחס למבקרים פנימיים, שכידוע אינם מתמקדים באימות ספרי החשבונות אלא מספקים להנהלה הבטחה בתחומים תפעוליים ואסטרטגיים, הטענה שהבלוקצ'יין ייתר את הצורך בהם היא חסרת יסוד.

בנוסף, לטובת מבקרי טכנולוגיות המידע שבינינו, יודגש כי אמינות הבלוקצ'יין מושפעת מהסביבה הטכנולוגית שבה היא פועלת. לדוגמה, אם מבצעים עסקה דרך הסמארטפון, הבלוקצ'יין אינו יכול להבטיח כי נתוני העסקה יהיו מוגנים מציתות או משיבוש על ידי צד ג' בעת הזנתם לסמארטפון. כך גם מערכות העזר כמו חוזים חכמים המחוברים אליו בממשק. כלומר הטכנולוגיה עצמה אינה חפה מסיכונים. נראה שיישומי בלוקצ'יין בארגונים (על הסיכונים הטמונים בהם), יהיו דווקא הזדמנות למבקרים למתן שירותי הבטחה מתקדמים ובעלי ערך.

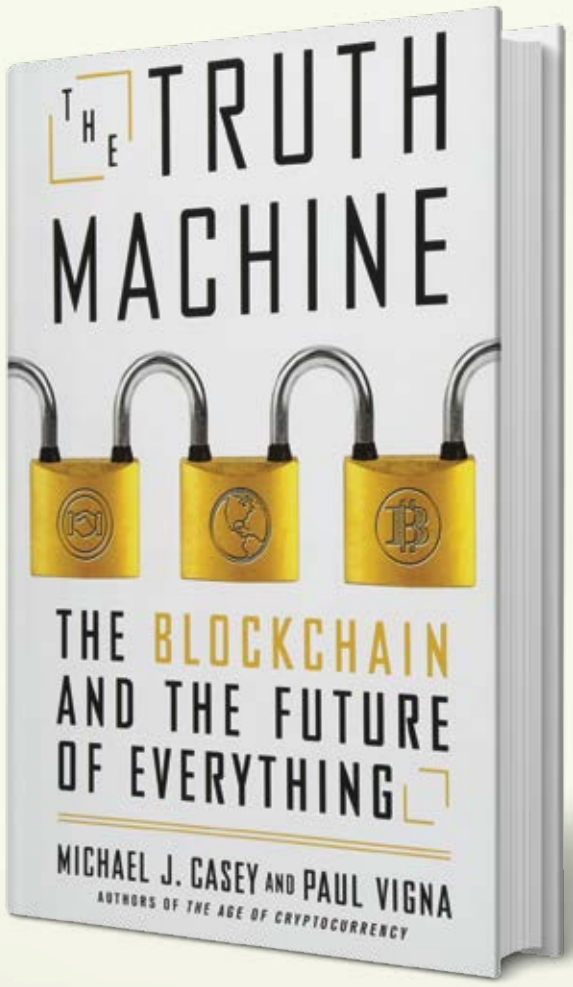
סיכום

האם קץ הביקורת אכן מתקרב? ניתן להניח כי בעתיד המוקדם או המאוחר מקצוע הביקורת כפי שאנו מכירים אותו אכן יעבור מן העולם, יחד עם מקצועות נוספים רבים של הצווארון הלבן, אבל הסיבה לכך לא תהיה בהכרח טכנולוגיית הבלוקצ'יין. סביר יותר כי ההתקדמות העצומה בתחומי הבינה המלאכותית והאנליטיקה היא שתוביל לעתיד שבו תוכנות ביקורת חכמות יחליפו את עבודת המבקר האנושי. עד שזה יתרחש, מומלץ ללמוד ולעקוב אחרי התקדמות הבלוקצ'יין דווקא כהזדמנות להרחבת מגוון שירותי ההבטחה והביקורת.

ספר מומלץ בתחום:

The Truth Machine:
The Blockchain and the Future of Everything

Vigna, Paul; Casey, Michael J.
St. Martin's Press (2018)



2018 FINANCIAL SERVICES
EXCHANGE
Connect. Collaborate. Evolve
Oct. 1-2, 2018
Washington, D.C.

GAM general audit management
CONFERENCE
WHERE LEADERS EVOLVE.
March 11-13, 2019
Gaylord Texan /
Dallas/Ft. Worth, TX

מניעת דלף מידע

מאת

ג'ני דניסוב | מנהלת פרויקטים - ביקורת פנימית, אמדוקס

מה זה דלף מידע (DATA LEAKAGE)?

בעידן שבו המידע נדרש לנוע באופן דינמי בתוך הארגון ומחוצה לו בערוצים רבים ומגוונים,

הסיכון שמידע רגיש יזלוג מתוך מערכות הארגון השונות למקורות שאינם מורשים גדל ומתעצם.

מידע רגיש עשוי לכלול מידע רפואי, מידע אישי ומידע עסקי ארגוני, נתוני כרטיסי אשראי, תשלומי לקוחות ועוד.

אירוע אבטחת מידע שבו מבוצעת פעולה כגון העתקה, העברה או צפייה במידע רגיש או מסווג, ללא הרשאה או בשגגה, מכונה אירוע דלף מידע.

בין אירועי דלף המידע הידועים ביותר ניתן למנות את פריצת אתר Ebay במאי 2014, שכתוצאה ממנה נחשפו 145 מיליון חשבונות של משתמשי האתר (כולל שמות, כתובות, תאריכי לידה וסיסמאות). כמו כן, ביולי 2017 דלף מידע אישי של 143 מיליון צרכנים אמריקאים עקב פריצת מערכות חברת Equifax על ידי האקרים.

ישנן אינספור דוגמאות נוספות של זליגת מידע רגיש, הן מחברות ענק עוצמתיות והן מארגונים בסדר גודל בינוני, המדגישות את הצורך של כל ארגון לשמור על שלמות, סודיות וזמינות המידע שברשותו בכל זמן נתון. מידע הוא אחד הנכסים החשובים ביותר של כל ארגון, ולכן על הארגון לפעול במיטב האמצעים העומדים לרשותו על מנת למנוע אירועי דלף מידע, בין היתר כדי למזער את הסיכונים לפגיעה במוניטין ואי עמידה בהוראות החוק והרגולציה.

בהתאם לממצאים העיקריים של סקר הנערך על ידי חברת Verizon Data Breach Investigations Report (DBIR) 2018, אירועי דלף מידע שמקורם בגורם חיצוני זדוני קטנו בשנה האחרונה (~73%) לעומת האירועים שנגרמו על ידי גורם פנים ארגוני (~28%).

מהם הגורמים העיקריים לדלף מידע?

הסיכונים להתרחשות אירוע דלף מידע מושפעים ממספר רב של גורמים שניתן לחלקם לקטגוריות הבאות:

גניבת מידע מהארגון על ידי גורם חיצוני

- גניבת מידע מהארגון ממניעים של ריגול עסקי, תוך שימוש בכלים טכנולוגיים כגון וירוסים וסוסים טרויאניים. לדוגמה פרשיית הסוס הטרויאני שהתגלתה בשנת 2004, כאשר שורה של חוקרים פרטיים שתלו תוכנת ריגול במחשבי חברות פרסום וחברות מסחריות גדולות במטרה לדלות מהם מידע לשם מכירתו למתחרים.
- גניבת מידע מהארגון תוך שימוש בגורם פנימי אנושי המופעל על ידי גורם חיצוני (כלומר הנדסה חברתית). הוצאת מידע מהארגון במקרה דנן עלולה להתבצע באמצעות קישור של מאגר המידע לרשתות חיצוניות, העתקת מידע מתחנות קצה למדיה נתיקה, ואף הוצאת מסמכים בתצורה קשיחה.
- דלף מידע מגורמים חיצוניים לגיטימיים, כגון ספקים, נותני שירות, חברות צד שלישי של הארגון, המחזיקים במידע רגיש - כתוצאה מאי יישום של אמצעי הגנה על המידע, כפי שמיושם בארגון עצמו. לדוגמה, דלף מידע מספקים כגון בתי דפוס, משרדי פרסום, עורכי דין, רואה החשבון והיועצים המשפטיים החיצוניים לארגון, שיש להם נגישות דיגיטלית למידע שבארגון.

זליגת מידע מהארגון בשוגג

- דלף מידע הנובע מתקלה או כשל טכני, טעויות אנוש או חוסר מודעות עובדים. לדוגמה, דלף מידע כתוצאה מטעויות הפצה של דואר אלקטרוני, קיום Metadata

בקובצי Office, אובדן מחשבים ניידים המכילים מידע עסקי רגיש, והיעדר היכרות של עובדי הארגון עם נהלים והיבטי רגישות המידע בארגון. דוגמה נוספת - עובד עלול להעתיק תוכן מסמך מסווג למסמך אחר בלי להיות מודע לכך שהתוכן מסווג, ולהוציא את המידע מחוץ לארגון ביודעין או בשוגג.

זליגת מידע מהארגון בזדון - על ידי גורם פנימי

- נוסף על כך, קיים סיכון כי עובד ממורמר, עובד שפוטר או עומד בפני פיטורים, או עובד שעתיד לעבור למתחרים, ינצל לרעה את הרשאות הגישה שלו למידע ויעביר אותו לגורמים חיצוניים.

דוגמאות לרגולציה בנושא מניעת דלף מידע

- חוק הגנת הפרטיות ותקנות אבטחת מידע המבוססות על חוק הגנת הפרטיות.
- GDPR - הרגולציה האירופית שנכנסה לתוקף ב-25 במאי 2018.
- הנחיות רשם מאגרי המידע.
- רגולציה פיננסית (הוראות המפקח על הבנקים, רשות שוק ההון, ביטוח וחיסכון).
- רגולציה ביטחונית בארגונים ביטחוניים/צבאיים.

כיצד ניתן להוריד את רמת הסיכון לדלף מידע בארגון?

ראשית, על הארגון לענות על שורה של שאלות מהותיות, לדוגמה:

- מהו המידע הקיים בארגון?
- כיצד הארגון מגדיר מידע רגיש ומהם רמות הרגישות השונות (לקבוע נוהל סיווג ותיוג מידע)?

  כך למשל, הנוהל האמור ימפה ויגדיר מהו הסיכון של מידע אישי לסוגיו; מהו הסיכון של מידע עסקי לסוגיו; מהו הסיכון של מידע פיננסי ומסחרי לסוגיו; מהו הסיכון של מידע טכנולוגי, כולל קניין רוחני, וכדומה.
- היכן המידע מאוחסן?
- מהם הערוצים שדרכם המידע עלול לדלוף?
- ולבסוף - כיצד למזער את הנזקים אם וכאשר יתרחש אירוע של דלף מידע?

במה להתמקד בעת ביצוע ביקורת בנושא מניעת דלף מידע?

1. **מדיניות ונהלים** - יש לבחון האם הוגדרו ומיושמים בארגון מדיניות ונוהלי אבטחת מידע בנושאי סיווג מידע, הפרדת סמכויות, זיהוי עובדים שחשופים למידע רגיש, גילוי וניהול אירועי דלף מידע, הדרכות, החלפת סיסמאות, בקרה שוטפת על הרשאות גישה תוך עדכונים עקב מעבר תפקיד או פרישה, נוהל באשר לעובדים העומדים בפני פיטורין, וכן נוהל בדבר אובדן/גניבת סלולרי או מחשב נייד המאפשר גישה.

2. **סקר דלף מידע** - מומלץ לבצע סקר דלף מידע מקיף על ידי גורם מומחה חיצוני ובלתי תלוי, במטרה לסקור את כלי אבטחת המידע שבהם הארגון עושה שימוש ולבחון את התאמתם לצורכי האבטחה העסקיים בארגון ושיטת העבודה הנהוגה בו. הסקר יאפשר לזהות את רמת התאימות בין כלי אבטחת המידע השונים ואופן הפעלתם אל מול הסיכונים לדלף מידע.

3. **מערך הרשאות** - יש לבחון כיצד מיושם מערך הרשאות וסמכויות במערכות המידע בארגון והאם הוא עומד בעקרון "הצורך לדעת" (Need to Know), תוך הגבלת הגישה למידע לבעלי התפקידים הזקוקים לו בלבד. כמו כן יש לבחון עמידה בעקרון הפרדת התפקידים. לדוגמה: עובדים הנחשפים למידע מסווג מתוקף תפקידם, עובדים הנחשפים למידע רגיש בסביבות "נמוכות" (כגון סביבת בדיקות, סביבת פיתוח) וגורמים חיצוניים (עובדי קבלן וכדומה). בנוסף, יש לבחון אילו בקרות מפצות יושמו על מערך ההרשאות, כגון הפצת דוחות חריגים על פעילות המשתמשים במערכות ובדיקתם.

4. **טכנולוגיה** - יש לבחון את הכלים הטכנולוגיים שהוטמעו בארגון לשליטה ומניעת דלף מידע בכל פעילות הארגון. פתרונות DLP – Data Leakage Prevention מאפשרים לשלוט ולהגביל את הוצאת הנתונים בנקודות הקצה בארגון. כך למשל, מערכות ה-UTM (Unified Threat Management) נחשבות לדור הבא של חומות האש (Firewalls), וכוללות יכולות סינון דואר אלקטרוני, סינון תכנים ובקרת יישומים.

5. **מודעות עובדים** - יש לבחון האם התוכנית להגברת המודעות של העובדים כוללת הסברה מספקת בנושאי אבטחת המידע הארגוני וחשיבות מניעת דלף המידע. לעובדים שמודעים לסכנות, לחוקים ולתקנות יש סיכון קטן יותר ליפול בשגגה לידי עברייני רשת.

6. **שילוב אבטחת מידע בתהליכי משאבי אנוש** - יש לבחון האם בקרות אבטחת מידע רלוונטיות שולבו גם בתהליכי משאבי אנוש, למשל: החתמת עובד חדש על נספח שמירת סודיות והנחיות אבטחת מידע, הבהרה לעובדים כי מבוצעים תהליכי ניטור ובקרה באופן תדיר אחר אירועי אבטחת מידע ודלף מידע מהארגון.

חמשת העקרונות לניהול סיכוני הונאות

מבוסס על התדריך FRAUD RISK MANAGEMENT GUIDE, שפורסם בשנת 2016 על ידי COSO

מאת

דני פרידמן | מבקר ראשי אמדוקס
דרור בר משה | סגן מבקר ראשי אמדוקס
פניני לרנר-מרלי | מנהלת פרויקטים - ביקורת פנימית אמדוקס

סקר להערכת הונאות שנערך בשנת 2016 שנערך על ידי ACFE Association of Certified Fraud Examiners - וכלל מעל 110 מדינות ובחינה של כ-2,400 מקרי הונאה, העלה כי ארגונים יאבדו בממוצע כחמישה אחוזים מהכנסותיהם השנתיות כתוצאה מהונאות.

סך כל ההפסד שנוצר במקרים שנבחנו עמד על יותר מ-6.3 מיליארד דולר, כאשר הפסד ממוצע למקרה אחד עומד על 2.7 מיליון דולר. שימוש לרעה בנכסי הארגון אפיין 83% מהמקרים, אולם הביא להפסד חציוני נמוך יחסית של 125 אלף דולר בלבד. לעומת זאת, הונאות בדוחות הכספיים של הארגון מאפיינים פחות מ-10% מהמקרים, אך ההפסד החציוני שגרמו נאמד בכ-975 אלף דולר. מקרי שחיתות נצפו ב-35% לערך מהמקרים עם הפסד חציוני של 200 אלף דולר.

עוד נציין כי ככל שההונאה מתבצעת על פני תקופה ארוכה יותר, כך הנזק הפיננסי והתדמיתי גדול יותר. בעוד שמשך זמן ההונאה החציוני שנרשם בסקר עמד על 18 חודשים עם הפסד חציוני של 150 אלף דולר, כאשר בחנו את מקרי הקצה של הסקר זוהו מקרי הונאה שהתרחשו במשך יותר מ-5 שנים וגרמו להפסד חציוני של 850 אלף דולר.

אין ספק שהעולם העסקי הופך למורכב יותר מיום ליום. לפיכך נדרשת נקודת מבט רחבה בבואנו לבחון וליישם תהליכים לניהול סיכונים בארגון כחלק מהממשל התאגידי שההנהלה אחראית לו. הדברים אמורים לגבי ניהול סיכונים בכלל וסיכוני הונאה בפרט.

פרסומי ה-COSO

בשנת 2013 פרסם ארגון ה-COSO את מודל הבקרה הפנימית Internal Control Integrated Framework.

המודל מספק שלוש קטגוריות של יעדים המאפשרים לארגונים להתמקד בהיבטים שונים של בקרה פנימית:

1. יעדים תפעוליים
2. יעדי דיווח
3. יעדי ציות.

לצידם קובע המודל את חמשת מרכיבי הבקרה הפנימית:

1. סביבת הבקרה
2. הערכת סיכונים
3. פעולות בקרה
4. מידע ותקשורת
5. פעולות ניטור.

מודל זה זכה לאימוץ ושימוש רב לאומי והוכר כמודל מוביל לעיצוב ויישום של בקרה פנימית ולהערכת האפקטיביות של הבקרה הפנימית.

המודל קובע 17 עקרונות המקושרים אל חמשת מרכיבי הבקרה הפנימית שתוארו לעיל, ומבהיר כיצד יש להבין, להשתמש ולהטמיע את מערכות הבקרה הפנימית בצורה אפקטיבית. הארגון מדגיש שעל מנת שמערכת בקרה פנימית תהיה אפקטיבית, כל אחד מ-17 העקרונות צריכים להתקיים ולפעול יחד באופן משולב.

העיקרון השמיני מבין 17 העקרונות שלהלן קובע שיש לבחון האם: "הארגון מתייחס לפוטנציאל להונאה בהערכת הסיכונים להשגת יעדיו".

Fraud Risk Management Guide, שפורסם על ידי COSO בספטמבר 2016, מפרט כיצד ניתן ליישם עיקרון זה הלכה למעשה.

הונאה מוגדרת כפעולה מכוונת או השמטה/מחדל, המיועדת להטעות אחרים ומובילה לגרימת הפסד לקורבן או רווח למועל.

מעבר למידע שנדרש כדי להעריך את הסיכון להונאות, מדריך ה-COSO מספק הנחיות המורכבות מחמישה עקרונות ונקודות מיקוד הנדרשים להקמת מסגרת לניהול סיכוני הונאות. המדריך גם מתאר כיצד ארגונים בגדלים וסוגים שונים יכולים להקים תוכניות משלהם לניהול אפקטיבי של סיכונים אלה.

המודל מציע ראייה רחבה, שלפיה האחריות חלה הן על הדרג התפעולי והן על מועצת המנהלים וההנהלה. בכך יוצר המודל אחריות מערכתית כלל ארגונית.

המדריך גם מכיל אינפורמציה חשובה למשתמשים שמטמיעים תהליך לניהול הסיכון להונאות, כגון תפקידים ואחריות, שימוש בניתוח מידע ונתונים, ופיקוח על ניהול הסיכון.

כעיקרון כל ארגון חשוף להונאות. אין אפשרות למנוע לחלוטין את הסיכון, אולם הטמעה של העקרונות המוצעים בתדריך עשויה להעלות את ההסתברות שהונאות יימנעו או יזוהו תוך זמן סביר ואף ייצרו אפקט הרתעתי.

יישום מודל COSO 2013 בניהול הסיכון להונאות

המודל מציע כי יישום העיקרון השמיני יהיה בהתאמה לחמשת העקרונות המופיעים לעיל במודל COSO 2013:

על פי המודל לעיל, חמשת העקרונות לניהול הסיכון להונאות הם:

סביבת בקרה
CONTROL)
(ENVIRONMENT

"הארגון מייסד ומתקשר תוכנית לניהול הסיכון להונאות אשר ממחישה את הציפיות של מועצת המנהלים וההנהלה הבכירה ואת מחויבותם לרמת יושרה גבוהה וערכים אתיים בנוגע לניהול הסיכון להונאות".

הערכת סיכונים
RISK)
(ASSESSMENT

"הארגון מבצע הערכה מקיפה של הסיכון להונאות כדי לזהות תבניות וסיכוני הונאות מסוימים, מעריך את הסבירות והמהותיות שלהן, מבצע אומדן של בקרות ההונאה הקיימות ומיישם פעולות לצמצום הסיכון השיורי להונאות".

פעולות בקרה
CONTROL)
(ACTIVITIES

"הארגון בוחר, מפתח ומיישם פעילויות בקרה למניעה וזיהוי הונאות כדי לצמצם את הסיכון של התרחשות אירוע הונאה או חוסר זיהוי בזמן סביר".

מידע ותקשורת
INFORMATION &)
(COMMUNICATION

"הארגון מייסד תקשורת להשגת מידע בדבר הונאות אפשריות ומאמץ גישה לתיאום לביצוע חקירה ופעולות תיקון כדי לטפל בהונאות באופן הולם ובזמן סביר".

פעולות ניטור
MONITORING)
(ACTIVITIES

"הארגון בוחר, מפתח ומבצע הערכות שוטפות כדי לוודא האם כל אחד מחמשת העקרונות לניהול הסיכון להונאות קיים ופועל, ומתקשר ליקויים בתוכנית לניהול הסיכון להונאות בזמן סביר לצדדים האחראים לנקיטת פעולות לתיקון, לרבות הנהלה בכירה ומועצת המנהלים".

כאמור, לכל אחד מחמשת העקרונות קיים פירוט לגבי אופן יישומו (נקודות למיקוד).
להלן דוגמה לנקודות למיקוד שיש לקחת בחשבון ביישום העיקרון הראשון (סביבת הבקרה):

- מחויבות הארגון לניהול הסיכון להונאות.
- תמיכה במנגנון פיקוח על הסיכון להונאות.
- כינון מדיניות מקיפה לניהול הסיכון להונאות.
- הגדרת תפקידים והאחריות ברחבי הארגון לפיקוח על הסיכון להונאות.
- תיעוד מדיניות ניהול הסיכון להונאות.
- תקשור ניהול הסיכון להונאות בכל דרגי הארגון.

גישה מקיפה זאת מזהה ומדגישה את ההבדל המהותי בין חולשות בבקרה הפנימית שעלולות להוביל ל"טעות" לבין החולשות שעלולות לאפשר "הונאות". ההבדל המהותי הוא הכוונה.

ארגון שמסתפק בהוספת הערכת הסיכון להונאות להערכת הבקרה הפנימית הקיימת, עלול שלא לבחון באופן יסודי ולזהות אפשרויות לפעולות מכוונות המיועדות ל:

- הצגה מוטעית של המידע הפיננסי.
- הצגת מוטעית של מידע לא פיננסי.
- מעילה בנכסים.
- מבצעי פעולות לא חוקיות או מושחתות.

סביר שגישה מקיפה זו תניב הערכה יעילה ומקיפה יותר של הסיכון להונאות.

> המודל לניהול סיכוני הונאות, מאפשר למבקרים הפנימיים להביא להנהלות ולדירקטוריונים גישה שיטתית ומעשית שניתן להסבירה וליישמה בפשטות.

נספחים הכלולים במדריך

במדריך ישנם נספחים רבים בעלי ערך רב, הכוללים בין היתר תבניות, כלים פרקטיים, מודלים ונהלים לדוגמה שיכולים לסייע רבות ביישום המודל הלכה למעשה. המדריך כולל: סקר לדוגמה לניהול הסיכון להונאות שתוצאותיו עשויות להדגיש את הנושאים שבהם כדאי להתמקד ביישום ניהול הסיכון; דוגמה לנוהל ניהול הסיכון להונאות; כלי מפורט (מבוסס אקסל) למיפוי והערכת הסיכון להונאות, ושלל כלים נוספים ותבניות.

הביקורת הפנימית וניהול הסיכון להונאות

מעורבות המבקרים הפנימיים בתהליכי העיצוב והיישום של ניהול הסיכונים בארגון עשויה להיות מאתגרת ביותר. מבקרים בעלי המיומנות והניסיון המתאימים, יכולים להוסיף ערך ולסייע להנהלה בעצם העלאת המודעות והדגשת החשיבות של ניהול הסיכונים להצלחת הארגון.

בכך ממלא המבקר הפנימי תפקיד מפתח כיועץ מהימן (Trusted Advisor) המסייע להנהלה בשיפור ביצועיה בכלל ובשיפור הממשל התאגידי בפרט.

סיכום

בעשורים האחרונים גובר הדיון בסיכונים העלולים לפגוע ביעדי הארגון ולפגום בפעילותו. על הרקע הזה גוברת חשיבות ניהול הסיכונים בכלל וניהול הסיכון להונאות בפרט.

תרומתה של הביקורת הפנימית היא בהוספת הערך ושיפור הבקרה הפנימית. המודל המוצע כאן ליישום מערך לניהול סיכוני הונאות, מאפשר למבקרים הפנימיים להביא להנהלות ולדירקטוריונים גישה שיטתית ומעשית שניתן להסבירה וליישמה בפשטות. כמו כן, המבקר הפנימי יכול לנצל את הידע הרב שצבר על התהליכים בארגון כדי לסייע בניהול הסיכון להונאות.

מבקרים פנימיים שיבחרו שלא להיות מעורבים בתהליך ניהול הסיכונים הארגוני, עלולים להחמיץ הזדמנות להוסיף ערך לארגון ולפתח קשר חזק יותר עם הדירקטוריון.

עמותה וקוץ בה?

סיכונים מרכזיים בארגוני המגזר השלישי

מאת

חני עמר | רו"ח, משפטנית, שותפה, RAS Group, BDO

בשל תרומתו הרבה של המגזר השלישי לחברה בישראל, הוא זוכה לאמון רב מצד הציבור, ומכאן החשיבות בכינון תרבות ניהול סיכונים מפותחת במגזר.

במאמר זה אסקור סיכונים מרכזיים הרלוונטיים עבור עמותות וארגונים אחרים ללא כוונת רווח בישראל, בדגש על אלו בסדרי גודל קטן עד בינוני (בעלי מחזור כספי שנתי של עד 10 מיליון ש"ח, המהווים את הרוב המוחלט של האלכ"רים בישראל), מתוך ההנחה הסבירה שבארגונים כאלה המשאבים המוקצים לבקרה ולניהול סיכונים נמוכים יותר.

רגולציה מתגברת

בעשור האחרון חלה התפתחות משמעותית ברגולציה החלה על האלכ"רים, הן מבחינה מהותית (ההוראות הוחמרו) והן מבחינה כמותית (תדירות וכמות העדכונים עלו בצורה משמעותית). מגמה זו עשויה להימשך וסביר להניח כי שינויים רגולטוריים נוספים עוד לפנינו.

ריבוי ההוראות והרגולטורים, אי ידיעה או חוסר הבנה של ההנהלה המתנדבת את המסגרת הנורמטיבית, היעדר מערכי ציות ואכיפה בקו ההגנה השני וסיבות נוספות, מעצימים את הסיכון להפרות רגולציה באלכ"ר.

בנוסף, רגולציה זו מהווה נטל על האלכ"רים, במיוחד עבור אלו הניצבים בפני מספר רגולטורים (החשב הכללי, רשויות המס, משרדי ממשלה שונים, וזאת לצד רשם העמותות כרגולטור המרכזי), ועולה החשש שהאלכ"ר לא יעמוד בקצב הדינמי של הרגולציה ולא יספיק להפנים את הדרישות החדשות.

דרכי התמודדות אפשריות:

- למפות היטב את הרגולציה החלה על הארגון ואת מעמדו מול כל רגולטור ולבנות את 'המפה הרגולטורית' של הארגון.
- לערוך סקר ציות כחלק מתוכנית הביקורת הפנימית.
- לכלול מתן הדרכות ומסירת מידע מהיועצים והמבקרים השונים במסגרת השירותים השוטפים המתקבלים מהם.

הנהלה מתנדבת

חברי הוועד המנהל וועדת הביקורת, חברי העמותה (האספה הכללית) ואורגנים חשובים אחרים הם מתנדבים בלבד, כלומר לא מדובר ב-"Day Job" שלהם.

הרגולציה המתגברת והיעדר דרישות רגולטוריות בעניין ההכשרה, ההרכב והכישורים של ההנהלה המתנדבת מעלים את הסיכון לחוסר בקיאות ומקצועיות של אורגנים חשובים. כפועל יוצא, עולה החשש שמוסדות ההנהלה והביקורת לא יבינו היטב את מסגרת אחריותם ואת הנדרש על מנת לממש אותה כראוי. חוסר הבנה של התפקיד ושל האמצעים שנדרשים על מנת למלא אותו בצורה אפקטיבית משליכים על רמת הממשל התאגידי בארגון, ועלולים להביא לכך שהאורגן שינהל את הארגון בפועל ויתווה את המדיניות יהיה המנכ"ל והכפופים לו ולא הגופים האמונים על כך (כלומר הוועד המנהל).

דרכי התמודדות אפשריות:

- למפות את המבנה הארגוני של האלכ"ר (העמותה/החל"צ) ולבחון אם אכן מתקיימים כל האורגנים כנדרש, תוך שמירה על יחסי הכפיפות והיעדר ניגוד העניינים הרלוונטיים.
- לבחון את תפקוד האורגנים השונים ולזהות נקודות חוזקה וחולשה בתפקודם.
- לערוך מדריך בסגנון 'ערכת כניסה לתפקיד' לחבר ועד מנהל או ועדת ביקורת חדשים, ולבנות תוכנית הדרכות והעשרה מסודרת לחברים.

סיכוני (היעדר) בעלות

בעמותה אין בעלי מניות, אלא מייסדים שהקימו את האלכ"ר לטובת מטרה מוגדרת, שכמובן אינה עשיית רווחים. בעמותות שבהן דור המייסדים כבר אינו פעיל והוועד המנהל מתחלף מדי תקופה, יוצא כי אין 'בעל בית' בצורה מובהקת ועולה החשש של היעדר 'רציפות שלטונית'. סיכון בעלות זה עלול להביא לחוסר יכולת להוביל מהלכים משמעותיים ארוכי טווח ולהיעדר גורם מרכזי המודד את התנהלות וביצועי האלכ"ר ביחס לחזונו וייעודו מקורי.

בנוסף, חשוב לזכור כי לעיתים ציבור מקבלי שירותי האלכ"ר פחות מגובש ומודע לזכויותיו, או שהוא עוקב במידה פחותה אחר ניהול ענייני האלכ"ר, שכן הוא אינו נהנה מרווחיו, ולכן אינו מתנהג כ'בעל עניין רגיל' ויתקשה לזהות פגיעה שמקורה בירידה באיכות השירות או המוצר.

בעמותות שבהן יש מספר חברים רב, הבעיה מחריפה עוד יותר. כמות גדולה של חברים והטרוגניות גבוהה ביניהם עלולות להביא לתופעה של חוסר מעורבות בנעשה בעמותה ("כי בטוח יש מישהו אחר שעושה את זה") ואף לחוסר אכפתיות.

דרכי התמודדות אפשריות:

- לקיים דיונים באורגנים המנהלים של האלכ"ר, במטרה לגבש את התמונה המלאה ולנסות לגבש 'מידע צופה פני עתיד' ולזהות את הסכנות הפוטנציאליות ולהיערך לקראתן.
- לזהות את 'הבעלים האמיתיים' של הארגון ולנסות לרתום שותפים איכותיים נוספים לדרך.

חוסר יציבות כלכלית

היקף פוחת של תרומות ומענקים, כפילות רבה בארגוני המגזר השלישי שמביאה לתחרות על קהל היעד, הפרטת שירותי הרווחה של המדינה (מכרזים), התייקרות המחיה, חוסר היכולת לגבות מחיר כלכלי מלא בעד השירותים ועוד, כל אלו מערערים את כרית הביטחון הפיננסית של הארגון. הארגון מחויב לאתר מקורות הכנסה נוספים ולנקוט שיטות יצירתיות להגדלת ההכנסה, לגבש תוכנית אסטרטגית לטווח הקצר והארוך, ולעיתים אף לקבל החלטות קשות אודות סגירת תוכניות ומתקנים. המצב מסוכן עוד יותר בעבור האלכ"רים הפועלים על פי חוזים ממשלתיים והופכים למעשה לסוכני הרווחה של המדינה, מפני שהם מאבדים את היכולת לגמישות ועצמאות כלכלית בהיותם תלויים במשרד שעמו הם התקשרו ובתקופת ההתקשרות.

זאת ועוד, תנאי אי הוודאות והלחץ שנוצר בעקבות זאת עלולים לייצר תמריץ לסטייה ולניצול לרעה של משאבי האלכ"ר (המוגבלים ממילא) כחלק מגיבוש דרכים יצירתיות לחולל שינוי.

במאמר מוסגר - פועל יוצא של חוסר היציבות יכול להיות תגמול נמוך של המנהלים באלכ"ר, דבר העלול לפגוע באיכות הניהול או במוטיבציה הארגונית.

דרכי התמודדות אפשריות:

- בדיקה שנתית ממוקדת של היחסים הפיננסיים של הארגון, זיהוי החסמים הכלכליים המהותיים, ובחינת הזדמנויות להתייעלות וחיסכון.
- קיום 'שולחן עגול' למנהלים בנושא הבטחת יציבות כלכלית ובניית תוכנית אסטרטגית לטווח הקצר והארוך.

סיכוני הלבנת הון

פריסה על פני אזורים גאוגרפיים שונים בארץ ו/או בעולם, הסתמכות על מתנדבים שלא עוברים בהכרח סינון/בדיקות רקע, קבלת כספי מזומן כתרומה מגורמים שאין איתם היכרות מוקדמת או ממקור לא שגרתי, גישה למקורות מימון שונים (מקומיים ובינלאומיים), אנונימיות התורמים ועוד, כל אלו עלולים להוות קרקע פורייה עבור גורמים עברייניים שרוצים לנצל את התשתית האלכ"רית על מנת להלבין את מקור הכספים או אפילו לכוון את משאבי האלכ"ר לטובת מימון טרור.

הרשות לאיסור הלבנת הון ומימון טרור פרסמה באוקטובר 2017 "דגלים אדומים" - אירועים העלולים להצביע על ניצול לרעה של האלכ"ר. כיום אין עוררין על כך שהעמותות והחל"צים בישראל צריכים לפתח מודעות לתרחישים ולסיכוני הלבנת הון/מימון טרור ולפעול בצורה אקטיבית על מנת לאתר פעילות מחשידה שעלולה לסכן את האלכ"ר כולו, לרבות בהיבטי תדמית ומוניטין.

דרכי התמודדות אפשריות:

- בדיקה לעומק של הליכי קבלת הכספים באלכ"ר והבקרות השלובות בהם, וניתוח הפוטנציאל לניצול לרעה של האלכ"ר לצורכי הלבנת הון/מימון טרור.
- פיתוח מודעות ארגונית (כולל הדרכות) לתרחישי ניצול לרעה ול"דגלים האדומים", והבניית דרכי הפעולה המצופות מבעלי התפקידים השונים בעת חשש לאחד מאלו.

סיכונים תפעוליים

למרות החשיבות שבהטמעת שיטות וכלי ניהול ובקרה מתקדמים, לא אחת קורה שאלו נדחקים לתחתית סדר העדיפויות באלכ"ר בשל הקושי בגיוס משאבים. שימוש בכלים ידניים או במערכות ממוחשבות מיושנות, הסתמכות רבה על ההון האנושי, וייתכן שאף פחדים מהטמעת מערכות מידע לתפעול ולניתוח נתונים, כל אלו יוצרים פתח גדול לטעויות בתכנון ובביצוע, ואף יותר מכך, פתח למעילות.

כמו כן, עמותות וחל"צים רבים משרתות אוכלוסיות פגיעות (ילדים, קשישים, בעלי מוגבלויות וכו'), והמתקנים של הארגון יכולים להיות ישנים או שלא בשליטתם (כגון מבנה המתקבל מהעירייה, פעילות בבתי ספר וכו'). תנאים אלו יוצרים סביבה בעלת פוטנציאל סיכון מיוחד, ודורשים הקפדה יתרה על כללי בטיחות וביטחון.

לצד אלו יש לקחת בחשבון גם את המידע הרגיש שייתכן שהאלכ"ר מחזיק אודות מקבלי השירותים - כתובות רגישות של דירות נערים בסיכון/מקלטים לנשים מוכות, מידע אודות סיוע משפטי שניתן על ידי העמותה וכו'. הארגון מחויב ליישם נוהלי אבטחה הולמים על מנת להבטיח שהמידע (הפיזי או הממוחשב) לא יזלוג החוצה, ועל מנת להבטיח שלא ייעשה בו שימוש לא ראוי בקרב גורמי העמותה הפנימיים.

דרכי התמודדות אפשריות:

- למפות את השירותים והתהליכים הקריטיים בארגון ואת מידת ההתאמה של מערכות המידע והכלים הניהוליים שבשימוש לתהליכים ולרמת ההגנה הנדרשת על המידע הרגיש.
- לזהות את נקודות התורפה העיקריות ולאפיין בקרות מפצות מתאימות.
- לבנות תוכנית מחשוב רב-שנתית (לרבות סדר עדיפויות ותקציב).
- לערוך סקר בטיחות וביטחון, לדרג את המפגעים, ולבנות תוכנית טיפול שתנוטר ותנוהל על ידי פורום בטיחות וביטחון ארגוני.
- לערוך ביקורות בנושאי בטיחות וביטחון, ואבטחת מידע פיזי ולוגי.

אמון רב בנושאי משרה מעטים

בארגוני מגזר שלישי רבים רווחת 'תופעה' של איוש משרות על ידי בעלי תפקידים קבועים לאורך זמן רב, במיוחד בתפקידי חשבות, כספים, רכש וכו', שלהנהלה יש בהם אמון רב, וזאת לצד מטה מצומצם.

הסיבות לכך הן רבות ונובעות מטעמים היסטוריים, פיננסיים, תפעוליים ועוד. בנוסף, היות שהאלכ"רים עוסקים לרוב במטרות בודדות ותחומות, הרי שנדרשים פחות בעלי תפקידים או שנדרש פחות גיוון בתפקידים השונים, כלומר אמון רב וסמכות רבה מופקדים בידי בעלי תפקידים מעטים. מצב ארגוני זה עלול לייצר הזדמנויות רבות יותר, ולו תיאורטית, לניצול לרעה של משאבי האלכ"ר על ידי בעלי התפקידים בארגון מכוח מעמדם ותפקידם בארגון ומכוח הוותק והניסיון שצברו.

דרכי התמודדות אפשריות:

- לערוך סקר סיכונים, לרבות איתור סיכוני מעילות והונאות.
- להעריך בביקורות הפנימיות את מרכיב סיכוני מעילות והונאות.
- לייחד בדוחות הביקורת פרק ייעודי בדבר הפרדת תפקידים וסיכונים שונים הנובעים מהמבנה הארגוני.
- שימוש במערך הקיים של טיפול בתלונות עובדים וציבור לניטור מידע מחשיד.

סיכום

המאמר סוקר סיכונים מרכזיים באלכ"רים קטנים ובינוניים. הסיכונים אינם מדורגים לפי חשיבותם או שכיחותם, ועל כל ארגון למפות היטב את הסיכונים הרלוונטיים אליו ואת עצימותם.

בארגונים אלו רצוי שהמבקר הפנימי באלכ"ר יראה את תפקידו גם כ'סוכן שינוי תרבות'.

חשוב מאוד שיפעל גם למען עידוד חשיבה ותרבות של ניהול סיכונים, למען הגברת המודעות לאירועי מעילות והונאות אפשריים, למען הגברת האפקטיביות הניהולית מצד ההנהלה המתנדבת, ולמען קידום תרבות ממשל תאגידי הולמת באלכ"ר.

סיכוני מודלים

הפעילות העסקית, המבקר הפנימי ומה שביניהם

מאת

מירב שפר | חטיבת הביקורת הפנימית, בנק לאומי

"INSTEAD OF GOING ON GUT FEELING, A COMPANY CAN INSTEAD ACT BASED ON DATA. BUT THIS REQUIRES THAT YOU CAN SIFT THROUGH THIS ENORMOUS AMOUNT OF INFORMATION TO FIND WHAT YOU NEED. SMART DATA TRIES TO DO JUST THAT, TO GIVE YOU THE RIGHT DATA AT THE RIGHT TIME."

אנדרס בורג, שר האוצר השוודי
(בין השנים 2006-2014)

רקע

כמות הנתונים שקיימים בעולם גדלה בשנים האחרונות בהיקפים עצומים. בכל רגע נוצרים פריטי מידע בדרכים שונות, ובהן מדיה חברתית, בלוגים, מיילים, תמונות ופעולות עסקיות.

כמות המידע והתפתחות הטכנולוגיה יוצרות לחברות עסקיות הזדמנויות באמצעות ניתוח הנתונים בשיטות סטטיסטיות מורכבות ובניית מודלים (BI; DATA ANALITICS). כבר היום נעשה שימוש רחב במודלים סטטיסטיים, כגון בקבלת החלטות על רכישת מוצרים ובבחירת חופשה משפחתית, על סמך מאפיינים הייחודיים לנו.

לצד ההזדמנויות העסקיות, בשימוש במודלים גלומים גם סיכונים העלולים להוביל להחלטות עסקיות או אסטרטגיות שגויות. לכן קיימת חשיבות לזיהוי סיכונים במודלים, להבנת המגבלות של המודלים ולניהול נכון של "סיכון המודלים". למבקר הפנימי יש תפקיד חשוב בבחינת שלמות ואפקטיביות מסגרת הבקרה שהארגון הגדיר בניהול סיכוני מודלים. עם זאת, קיימות מספר דילמות והתלבטויות בנוגע לאופן יישום הביקורת, כפי שיפורטו בהמשך המאמר.

מהו "מודל" ומהם "סיכוני מודל"?

באפריל 2011 יצאה הנחיה מעודכנת המשותפת ל-OCC (המשרד לפיקוח על המטבע במשרד האוצר האמריקאי) ול-FED (הבנק המרכזי בארה"ב), המגדירה מודל כך:

מודל הוא שיטה כמותית, מערכת או גישה המתייחסת לתיאוריות, טכניקות והנחות סטטיסטיות, כלכליות, פיננסיות או מתמטיות, שבו מעובדים נתוני קלט לצורך קבלת אומדנים כמותיים.

מודלים העונים להגדרה זו עשויים לשמש לניתוח אסטרטגיות עסקיות, ליווי החלטות עסקיות, זיהוי ומדידה של סיכונים, הערכת חשיפות, ביצוע מבחני קיצון, הערכת נאותות הון, ניהול נכסי לקוחות, מדידת ציות למגבלות פנימיות, ועמידה בדרישות הדיווח הכספי או הרגולטוריות. הגדרת המודל מתייחסת גם למקרים שבהם הנתונים עצמם מבוססים על הערכת מומחה, ובלבד שהמידע המופק מהמודל הוא כמותי.

הגדרה זו היא רחבה מאוד וכוללת כלים שונים לקבלת החלטות, כל עוד התוצר הוא כמותי.

בהתאם להנחיה שלעיל, "סיכון מודל" מוגדר כפוטנציאל לנזק הנובע מהחלטות המבוססות על תוצרי מודל לא נכונים או שנעשה בהם שימוש לא נכון. "סיכון המודל" עלול להוביל להפסד כספי, לקבלת החלטות עסקיות ואסטרטגיות שגויות, או לגרימת נזק למוניטין של ארגון בנקאי.

לשם המחשה של גורמי הסיכון המרכזיים:

1. **טעויות במודל עצמו (להלן "קוד המודל") ובתוצריו** - לדוגמה, פיתוח מודל להצעות שיווקיות המבוסס על הנחות שגויות לגבי העדפות הצרכנים; קבלת החלטה שגויה לגבי משתנים שייכללו במודל.
2. **שימוש שגוי בתוצרי המודל** - שימוש בתוצרי מודל למטרות אחרות מאלה שפותח עבורן. למשל, מחקרים הוכיחו כי שומן גורם לכולסטרול ולמחלות לב. למניעת מחלות לב ניתנו לחולים תרופה להפחתת כולסטרול, בעוד שלא הוכח כי הפחתת הכולסטרול עצמה מונעת מחלות לב. כתוצאה מכך חל גידול במוות ממחלות לב באוכלוסיית האנשים עם כולסטרול נמוך.

ניתן לצמצם את סיכון המודל על ידי קביעת תהליכים לפיתוח, תיקוף וניהול מודלים.

הנחיות בנושא תיקוף מודלים פורסמו על ידי האיחוד האירופאי כחלק מ- Solvency II Directive. כמו כן ועדת באזל הפיצה הנחיות בנושא במסגרת BASEL III.

גם בישראל, באוקטובר 2010 אימץ בנק ישראל את הנחיית ארגון ה-OCC משנת 2000 בנושא תיקוף מודלים.

ניהול סיכון מודלים ותפקיד המבקר בבדיקת איכות ניהול הסיכון בכללותו ברמת המודל הבודד

בהתאם לפרקטיקה המקובלת, ניהול "סיכון המודלים" מושתת על שלושת קווי ההגנה כמתואר בתרשים:

תפקיד המבקר הפנימי בבדיקת קוד - דילמות:

ביקורת פנימית מתמקדת, בין היתר, בבדיקת תהליכי עבודה וקיומן של בקרות הולמות ומספקות שמטרתן לתת מענה לסיכונים הגלומים בתהליך.

בהתאם לכך, הביקורת הפנימית צריכה לבצע שני סוגי ביקורת:

1. בדיקת האפקטיביות של מסגרת הבקרה של ניהול סיכון המודלים ואופן יישום המדיניות.
2. ביקורת פרטנית ברמת מודל. בחירת המודלים שייבדקו תהיה בהתאם להנחיות רגולציה, ממשל תאגידי, רמת החשיבות לארגון וכדומה.

סוגיות שעלו בבדיקת מודלים:

בביקורות שערכנו נתקלנו במספר סוגיות. את התשובות לחלקן למדנו תוך כדי תהליך הביקורת, ואנו עדיין בתהליך למידה:

א. האם המבקר הפנימי צריך לבדוק את איכות המודל עצמו ("קוד המודל")?

התפקיד המסורתי של מבקר פנימי הוא בדיקת תהליכי עבודה ובקרה לניהול הסיכונים המרכזיים בנושא המבוקר, הנותנים מענה לתיאבון הסיכון והמדיניות שהוגדרו על ידי הדירקטוריון וההנהלה הבכירה. בדיקת איכות קוד המודל עצמו, לרבות שיטות סטטיסטיות שנבחרו על פני חלופות אפשריות, עלולה להתפרש כבדיקת טיב החלטה ולא רק דרך קבלתה.

מצד שני - ישנה מגמה הולכת וגוברת להפיכת תהליכי עבודה לאוטומטיים, תוך הסטת הפעילות לאפיקים דיגיטליים, בלי שקיימת מעורבות של גורם אנושי בתהליך. לכן המערכות המיכוניות והמודלים מקבלים משנה חשיבות בתמיכתם בניהול הפעילות העסקית, וחשוב שהמבקר הפנימי יבדוק את איכות המערכות המיכוניות והמודלים. להערכתנו, היעדר התייחסות לטיב מודלים עלול לפגום באפקטיביות הביקורת הפנימית. לפיכך נשאלת השאלה הבאה - האם יש בכך בדיקת טיב ההחלטה? ואם כן, האם מדובר בביקורת או בייעוץ?

חשוב לציין: בדיקת קוד המודל אינה מוגבלת רק לנוסחה המתמטית אלא מחייבת הבנה של השימושים העסקיים. בדיקת קוד המודל בלי שקיימת הבנה של השימושים העסקיים היא חלקית ולא מספקת.

ב. בדיקת קוד מודל - ביקורת או ייעוץ?

הנחיית ה-OCC משנת 2011 דורשת כי בדיקת מודל תיעשה על ידי עובדים בעלי ידע ומומחיות בתחום. מאחר שבדיקת קוד המודל היא מקצועית במהותה, שימוש במומחים בעלי ידע ייחודי העלה אצלנו חשש שביצוע הביקורת בנושא יימצא בתחום האפור שבין ביקורת לייעוץ.

היות שעבודת הביקורת המסורתית אינה כוללת מתן ייעוץ, ומאחר שבביצוע מטלת ביקורת, המבקר הפנימי מתמקד בבדיקת תהליכי עבודה בהתייחס לסיכונים הגלומים בהם,

הרי שלדעתנו על המבקר לזהות רק את הסיכונים הטמונים בניהול המודל ולבדוק אם נקבעה מסגרת בקרה הנותנת מענה לסיכונים אלה.

מכאן, שליקויים שמעלים מומחי הביקורת בהתייחס לטיב קוד מודל ומגבלותיו, עשויים להצביע על ליקויים בתהליך קבלת ההחלטות בנוגע לבחירת סוג המודל, אופן יישומו, ממשקי העבודה בין יחידת הפיתוח והתיקוף וכו'. כלומר, הליקוי שנמצא בטיב המודל הוא הדוגמה להתממשות הסיכון בתהליך העבודה.

ג. עומק הבדיקה ומומחיות המבקרים כפונקציה של ניהול סיכונים וניהול משאבים

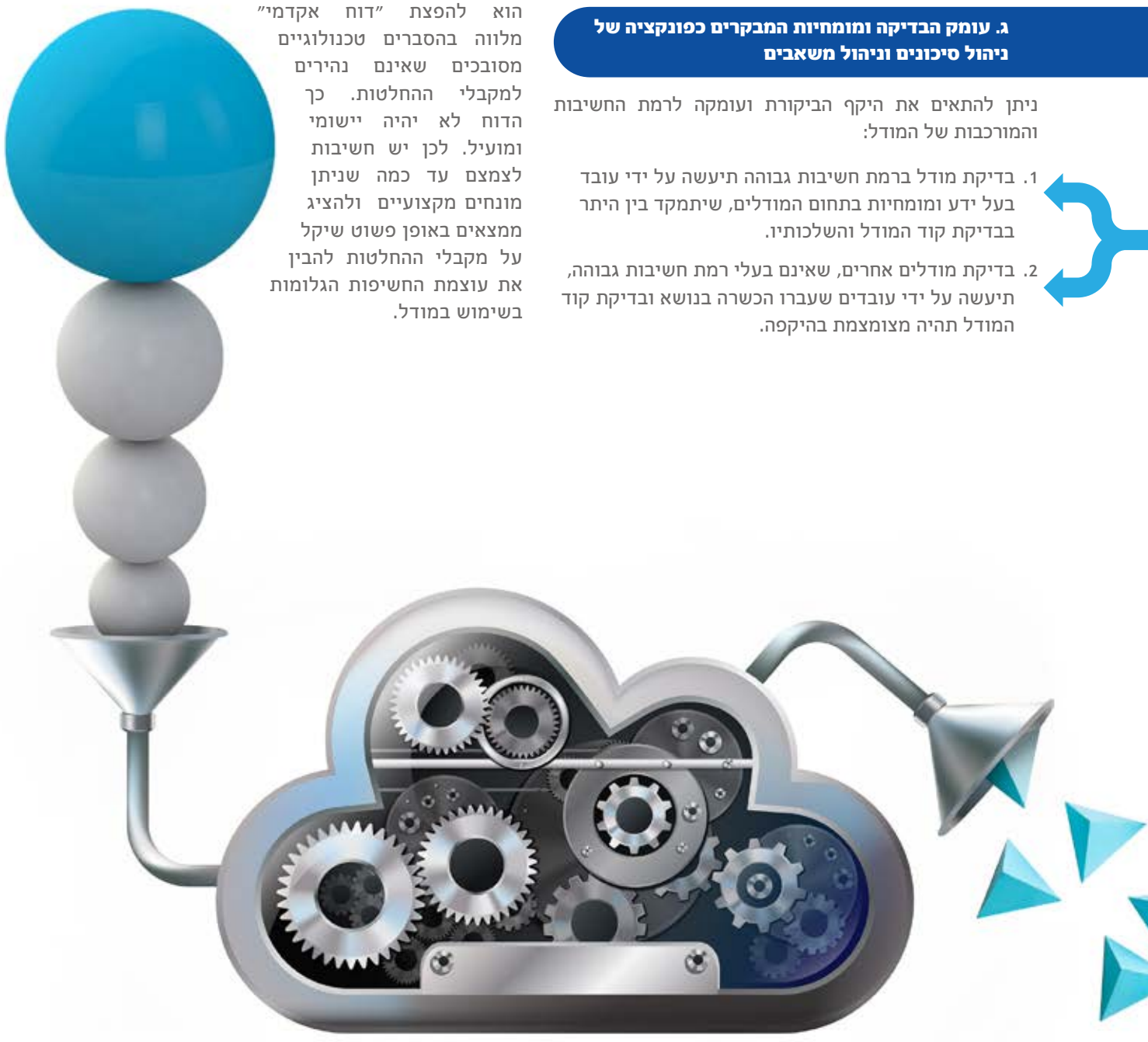
ניתן להתאים את היקף הביקורת ועומקה לרמת החשיבות והמורכבות של המודל:

1. בדיקת מודל ברמת חשיבות גבוהה תיעשה על ידי עובד בעל ידע ומומחיות בתחום המודלים, שיתמקד בין היתר בבדיקת קוד המודל והשלכותיו.
2. בדיקת מודלים אחרים, שאינם בעלי רמת חשיבות גבוהה, תיעשה על ידי עובדים שעברו הכשרה בנושא ובדיקת קוד המודל תהיה מצומצמת בהיקפה.

כך או כך - ניתן לאתגר את תוצרי המודל והשימוש בהם מבחינה עסקית. לדוגמה, ניתן להשוות את תוצרי המודל לתוצרים של מערכות אחרות המפיקות מידע זהה או דומה. בהיעדר זהות בתוצרים של כלים שונים לניהול הסיכון, הרי שהדבר יכול להעיד על בעיתיות באיכות קוד המודל.

ד. תוצר הביקורת - חשיבות לפישוט

מדובר בנושא מורכב, כאשר החשש הוא להפצת "דוח אקדמי" מלווה בהסברים טכנולוגיים מסובכים שאינם נהירים למקבלי ההחלטות. כך הדוח לא יהיה יישומי ומועיל. לכן יש חשיבות לצמצם עד כמה שניתן מונחים מקצועיים ולהציג ממצאים באופן פשוט שיקל על מקבלי ההחלטות להבין את עוצמת החשיפות הגלומות בשימוש במודל.



דגשים מרכזיים בעת בדיקת מסגרת הבקרה הכוללת לניהול "סיכון מודלים"

1. בדיקת תוכנית העבודה של הארגון לפיתוח ותיקוף מודלים.
2. בדיקת משך הזמן לפיתוח מודלים.
3. אפקטיביות מנגנוני הדיווח לדירקטוריון ולהנהלה הבכירה.
4. קשרי הגומלין בין היחידות השונות בתהליך.
5. אפקטיביות ניהול קטלוג המודלים.
6. שלמות נוהלי העבודה.

דגשים מרכזיים בעת בדיקת מודל ספציפי

רכיב הקלט

1. בדיקת מסגרת הבקרה: בדיקת שלמות ומהימנות הנתונים המוזנים למודל.
2. קביעת תהליך הטיפול והבקרה בנוגע לנתונים חסרים.

ממשל תאגידי

1. קיום דיונים בהנהלה הממונה באשר לפערים שאותרו בתהליך תיקוף המודל.
2. קיום תהליך תיקוף בלתי תלוי במסגרת תהליך הפיתוח.
3. טיפול שיטתי ומקיף בפערים שעלו במסמכי התיקוף.
4. בחינת שלמות תיעוד המודל, לרבות הנחות ושיקולים בקבלת החלטות בשלבים השונים של פיתוח המודל.
5. קיום תהליכי תיקוף תקופתיים שקטלוג המודלים הגדיר מראש ושלמות מסמכי התיקוף.
6. תקינות ממשקי העבודה בין הגורם המפתח לגורם המתקף.

רכיב העיבוד

1. קיום תהליכי ניהול שוטפים של המודל, לרבות: הרצת בחינה תקופתית של שרידות כושר הניבוי של המודל.
2. קיום תהליך לבחינת שינויים רגולטוריים ועסקיים שחלו על כושר הניבוי של המודל ובחינת הצורך בהתאמת המודל לשינויים אלה.
3. בדיקת קוד המודל על ידי עובד בעל ידע ומומחיות/מיקור חוץ. הבדיקה תבחן את תהליך הפיתוח, ובכלל זה:
   - תהליך פיתוח קוד המודל, לרבות השיקולים בקביעת ההנחות המרכזיות ואופן יישומן.
   - אופן הטיפול הכולל בנתונים.
   - התאמת המודל לנתונים.
   - קיום תהליך לקביעת המדדים שיבחנו את כושר הניבוי של המודל.
   - אתגור המודלים הקיימים במודלים מתחרים, תוך **בחינת שימושים ודוחות פלט**.
4. קיום תהליכי בקרה לבחינת סבירות תוצאות המודל טרם העברתם לגורם העסקי.
5. בחינת אפקטיביות השימוש בתוצרי המודל. אתגור תוצאות/שימושי המודל מול הפעילות העסקית.

סיכום

מודלים מהווים כלי מרכזי בתהליכי קבלת החלטות בפעילויות הליבה של תאגידים עסקיים, פיננסיים ואחרים. לצד בדיקת ניהול סיכון המודל בכללותו, יש לשלב בתוכנית העבודה הרב שנתית ביקורות ברמת מודל בהתחשב ברמת החשיבות של המודל לארגון ותמיכתו בפעילות העסקית.

אפקטיביות הביקורת ברמת מודל טמונה ביכולת של המבקר להעריך את מידת התמיכה של המודל בפעילות העסקית, בהתאם למטרות שהוגדרו מראש. במילים אחרות - היכולת לכמת את הליקויים/חשיפות שאותרו בקוד המודל על הפעילות העסקית הינה האתגר המרכזי העומד לפתחו של המבקר.

הונאות בדיווח כספי – כיצד ניתן להתמודד עם הסיכון?

מאת

שי מדינה | רו"ח, שותף, מנהל מחלקת ביקורת חקירתית, פאהן קנה ניהול בקרה בע"מ

ברק ציפרוט | מנהל תחום גופים מוסדיים, פאהן קנה ניהול בקרה בע"מ

לאחרונה פורסם כי ניתוח ראשוני שנערך על ידי נאמני חברת הוניגמן מצביע על כך שערכי המלאי שהוצגו בספרי החברה בשנים האחרונות, כמו גם אלה שהוצגו על ידי החברה בבקשת הקפאת ההליכים, לא תואמים את המציאות. לדברי נאמני החברה: "בירורים ראשוניים שערכנו מעלים חשש לניפוח, לכאורה, של נכס המלאי במאזנים, שהביא להגדלת שורת הרווח בספרים".

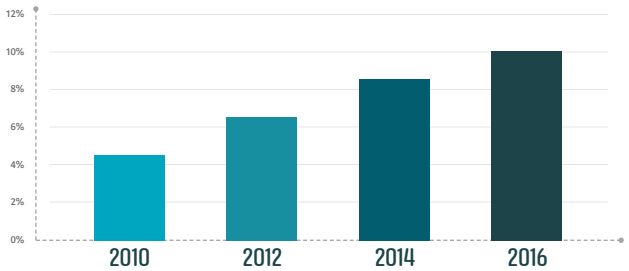
בחודש יוני 2015 נחשפנו לרישום כוזב בספרי חברת הבת נגב קרמיקה, רישום שהשפיע על הצגת הסעיפים השונים בדוחות הכספיים וגרם ל"ניפוח" רווחי החברה בכ-62 מיליון שקל.

פרשיות אלו הן רק קצה הקרחון של אירועי הונאות חשבונאיות בדיווח הכספי של חברות ציבוריות שנחשפו בשנים האחרונות. אירועים אלו מעלים ספקות בנוגע למידת התאמתם של מנגנוני הבקרה האמורים לאתר ולמנוע תרחישי הונאות חשבונאיות. ייתכן שאוזלת היד בנושא נובעת מהעובדה שהחברות לא השכילו להבחין בין מנגנוני הבקרה שיש ליישם כדי למנוע מעילות עובדים לבין אלו שבאפשרותן למנוע תרחישי הונאות חשבונאיות.

המצב בעולם ובארץ

בסקר בינלאומי שנערך על ידי איגוד בוחני ההונאות העולמית (ACFE) ופורסם בשנת 2016, שבמסגרתו נבדקו אירועי הונאות, מעילות ומעשי שחיתות שנחקרו במדינות שונות ברחבי העולם, נמצא כי קיים גידול בשיעור ההונאות החשבונאיות מבין כלל האירועים שנחקרו.

להלן גרף המציג את הגידול בשיעור ההונאות בדיווח הכספי בשנים 2010-2016:



בארץ המצב חמור עוד יותר. בשנת 2016 נערך סקר על ידי מחלקת הביקורת החקירתית של פירמת רו"ח "פאהן קנה ניהול בקרה", שבמסגרתו נבדקו עשרות אירועי הונאות, מעילות ומעשי שחיתות בענפי פעילות שונים. מהממצאים עלה כי בכ-16% מהמקרים היו אירועי הונאות בדיווח הכספי.

נתונים אלו מצביעים על הצורך בנקיטת צעדים אקטיביים במטרה לחשוף הונאות בדיווח כספי. במאמר זה נציג מספר דרכים ושיטות להתמודדות עם הסיכון.

סוגי ההונאות הנפוצות ביותר בדיווח כספי

להלן סוגי ההונאות הנפוצות ביותר בדיווח כספי, כפי שעולה מנתוני הסקר הבינלאומי שנערך על ידי לשכת בוחני ההונאות העולמית:

מסקרים שנערכו לאחרונה עולה תמונת מצב מדאיגה בכל הנוגע לגידול בשיעור מקרי ההונאות החשבונאיות.

• ביצוע מניפולציות בסעיפי התחייבויות והוצאות על ידי שימוש בהפרשי עיתוי, במטרה להשפיע על התוצאות הכספיות באמצעות דחיית הוצאות. לדוגמה, הפחתה

מלאכותית של הוצאות החברה השוטפות על ידי היוון הוצאות שוטפות לרכוש קבוע, לרבות היוון הוצאות לנכס שכבר הופעל. בדרך זו ההשפעה של ההוצאה על הדוחות הכספיים נפרשת על פני שנים במקום על התקופה החשבונאית הרלוונטית.

- הכרה בהכנסות שלא בהתאם לתקנים חשבונאים מקובלים - ייפוי הדוחות מבוצע על ידי הכרה בהכנסה טרם זמנה, רישום פיקטיבי של מכירות וביטולן בתחילת שנת הכספים הבאה, ורישום מכירות פיקטיביות בין חברות בקבוצה (פעולות מסוג זה אינן משפיעות על הדוחות הכספיים המאוחדים של קבוצת החברות אלא על דוחות הסולו של כל אחת מהחברות).
- עדכון שווי נכסי החברה באופן מלאכותי - כך לדוגמה, אחת הדרכים הנפוצות לייפוי הדוחות הכספיים היא "ניפוח" ערך המלאי (בין אם על ידי עדכון כמות פרטי המלאי במערכות התפעוליות ובין אם על ידי התערבות מלאכותית בערכים הכספיים של פרטי המלאי), המשפיע על מאזני החברה ועל תוצאות פעילותה.

כלי הבקרה הנהוגים כיום למניעת הונאות בדיווח כספי

מרבית המבקרים הפנימיים אינם נוהגים לכלול בתוכנית העבודה נושאים הקשורים לסיכוני הונאות בדיווח הכספי, מתוך הנחה כי נושאים אלו מטופלים במסגרת עבודת ה-SOX ומבוקרים על ידי רואה החשבון המבקר. אולם שיעור הגידול באירועי הונאה מעלה ספקות בנוגע להתאמתם של מנגנוני הבקרה אשר היו נהוגים עד כה.

המתודולוגיה המסורתית ליישום ה-SOX נועדה לוודא שלא קיימות טעויות מהותיות בדוחות הכספיים, אך מתקשה בזיהוי ואיתור של הטעיות מכוונות, ולכן מתקשה בזיהוי הונאות בדיווח כספי. להלן מספר סיבות לכך:

מאפיין	מה נדרש	מה מקובל במסגרת ה-SOX
מדגמים	שיטות דגימה מורכבות המסתמכות על כריית נתונים וניתוח חריגים.	שיטות דגימה אקראיות.
היקף בדיקות	בדיקת אוכלוסיות שלמות באמצעות הגדרת סקריפטים ושימוש בכלים ממוחשבים.	מדגמים קטנים באופן יחסי הנעים בין מקרים בודדים לעשרות מקרים בלבד.
ביצוע הבדיקות	בדיקות המבוססות תרחישים ומבוצעות על ידי מערכות ייעודיות לניתוחי נתונים לצורך זיהוי חריגים.	בדיקות ידניות המבוצעות על ידי גורם אנושי.
תלות	ביצוע בדיקות על מסדי נתונים שלמים באי-תלות מוחלטת בגורם העסקי.	לרוב הבדיקות תלויות בגורם העסקי שיספק את האוכלוסיות ואת המסמכים הרלוונטיים לבדיקה.
גורם ההפתעה	בדיקות חדשות ומגוונות שמפתיעות את הגורם העסקי.	בדיקות חוזרות ונשנות המבוצעות בכל שנה, דבר המוביל לכך שהנהלת הארגון מודעת לאופן וסוג הבדיקות ואף מתכוננת אליהן.
כפיפות ארגונית	כפיפות ארגונית שאינה יוצרת ניגודי עניינים, כגון כפיפות למבקר הפנימי/מנהל הסיכונים/ועדת הביקורת.	לרוב הכפיפות הארגונית היא לממונה על הכספים בחברה, אף שהונאות חשבונאיות מבוצעות לרוב על ידי הנהלת החברה, תוך מעורבותם או לכל הפחות ידיעתם של מנהלי הכספים.
מיומנות	עובדים מיומנים ומנוסים בזיהוי מעילות והונאות ושימוש בכלים ממוחשבים.	ידע מוגבל בזיהוי מעילות והונאות ושימוש בכלים ממוחשבים.

ההבדל בין הונאה חשבונאית למעילה או למעשה שחיתות:

הונאות חשבונאיות

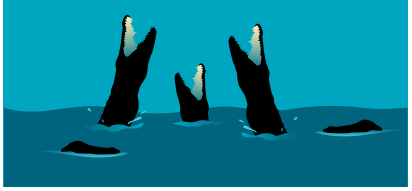
הונאות המבוצעות על ידי הנהלת הארגון כלפי גורמים חיצוניים, בעיקר לצורך שימור מעמדו של הארגון. הונאות מסוג זה כוללות מצגים מעוותים, בכוונת זדון, של מצבו הכספי של הארגון, במטרה להונות את ציבור המשקיעים ו/או גורמים הנמצאים בקשר עסקי עם הארגון. הונאות מסוג זה דורשות רמה גבוה של מורכבות, תחכום וטכניקות הסוואה משוכללות משום שמדובר בסכומי עתק (בדרך כלל מאות אלפי ש"ח לא ישפיעו על שווי החברה).

מעילת עובדים

פעולה של גורמים פנימיים, לעיתים בשיתוף פעולה עם גורמים חיצוניים, הפוגעת בנכסיו ובמצבו הכספי של הארגון.

שחיתות

שימוש לרעה על ידי בעל תפקיד/מקבל החלטות בסמכויותיו על מנת להשיג טובות הנאה או רווח אישי.



התפתחויות כלי הבקרה

בשנים האחרונות אנו עדים להתפתחות כלי הבקרה למניעת מעילות: מנהלי סיכונים עורכים סקרי סיכוני מעילות, ומבקרים פנימיים משלבים התייחסות לנושא בתוכנית העבודה של הביקורות הפנימית, תוך הסתייעות באנשי מקצוע המתמחים בתחום הביקורת החקירתית. למרות האמור,

נושא ההונאות בדיווח כספי נותר פעמים רבות מחוץ לתוכניות העבודה של המבקר, על אף שהמתודולוגיות הרלוונטיות ליישום SOX ולביקורת על דוחות כספיים מורות על כך.

בספטמבר 2016 פרסם ארגון ה-COSO מדריך בנושא מניעת הונאות ומעילות, המדגיש את מחויבות הארגון לנקוט גישה אקטיבית לצורך מניעת הונאות ומעילות. המדריך הוא חלק בלתי נפרד מעיקרון 8 ב-COSO 2013, שהוא המתודולוגיה המקובלת כיום לבחינת הממשל התאגידי במסגרת ה-SOX. להלן מספר נקודות שבהן עוסק המדריך:

1. קביעת תוכנית לניהול סיכוני הונאה במסגרת הממשל הארגוני.
2. ביצוע הערכת סיכונים מקיפה להונאות ומעילות.
3. פיתוח ויישום בקרות מונעות ומאתרות לזיהוי הונאות ומעילות.
4. קביעת מנגנון דיווח שיאפשר מסירת מידע בנוגע להונאות ומעילות שהתגלו.
5. פיקוח על תהליך ניהול סיכוני ההונאות והמעילות, שיאפשר הסקת מסקנות, הפקת לקחים ושיפור תהליכים.

במתודולוגית העבודה החדשה הנדרשת על ידי ארגון ה-COSO והמועצה לפיקוח על ביקורת דוחות כספיים בחברות ציבוריות – PCAOB (Protecting Investors through Audit Oversight), ניתן דגש בין היתר לנושאים הבאים:

- בדיקת אוכלוסיות שלמות באמצעות שימוש בכלים ממוחשבים ושיטות דגימה מורכבות המסתמכות על כריית נתונים וניתוח חריגים.
- בדיקות המבוססות על תרחישי הונאות ומעילות פוטנציאליות הרלוונטיות לאופי הארגון ולתהליכי העבודה המבוצעים בו.
- כפיפות ארגונית שאינה יוצרת ניגודי עניינים וביצוע בדיקות על מסדי נתונים שלמים באי-תלות מוחלטת בגורם העסקי.

מעיון בפרסומים החדשים עולה כי הטיפול בהונאות בדיווח כספי נופל בין הכיסאות. בעוד שארגוני ה- COSO וה- PCAOB מטילים את האחריות למניעת תרחישי הונאות ומעילות על גורמי הביקורת והבקרה השונים (כגון המבקרים הפנימיים, מנהלי הסיכונים וכו'), פעמים רבות שומרי הסף אינם כוללים בתוכניות העבודה למניעת מעילות בדיקת תרחישי הונאות בדיווח כספי, מתוך הנחה כי נושא זה מטופל במסגרת ה-SOX ועל ידי רואה החשבון המבקר.

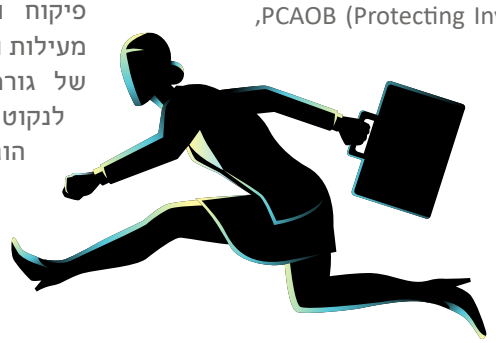
ניתן לאתר ואף למנוע את תרחישי ההונאות על ידי הטמעת בקרות תהליכיות ותקופתיות בארגון. לדוגמה:

ניתן לאתר ואף למנוע את תרחישי ההונאות על ידי הטמעת בקרות תהליכיות ותקופתיות בארגון.

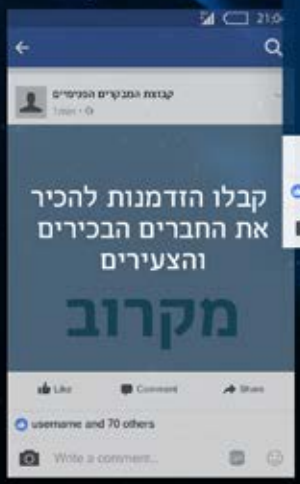
- יצירת ממשק אוטומטי בין המערכת הלוגיסטית המשמשת את החברה לצורך ניהול המלאי לבין המערכת הפיננסית, וזאת כדי לצמצם את האפשרות לביצוע פעולות ידניות העשויות להשפיע באופן מלאכותי על הרישומים החשבונאיים של החברה.
- ביצוע ביקורות תקופתיות המתמקדות בניתוח רישומים חשבונאיים חריגים, כגון פעולות המשפיעות באופן מלאכותי על סעיפי חתך.

סיכום

לנוכח התפשטות התופעה ולצורך התמודדות עם סיכוני הונאות ומעילות, נראה כי על חברות למסד מנגנוני פיקוח ובקרה שמטרתם איתור ומניעה של מעילות והונאות, לצד עריכת ביקורות תקופתיות של גורמים מקצועיים בתחום. על הארגונים לנקוט גישה אקטיבית שמטרתה לחשוף הונאות ומעילות בגוף המבוקר, גישה הכוללת בחינת תרחישי מעילות לצד תרחישי הונאות בדיווח הכספי על אף המורכבות שבכך, במסגרת תוכנית מתמשכת למניעת הונאות ומעילות.



הצטרפו לקבוצות דיון בפייסבוק ובלינקדאין



יש לכם שאלה?
שאלו אותנו ברשת

הקבוצה פתוחה לכל המבקרים הפנימיים

הצטרפו אלינו!

Daga
GRAPHIC DESIGN STUDIO

www.daga.co.il | office@daga.co.il | 077-5044740/1

מיומנה של מבקרת פנימית

תקן 2420 – מהי בדיוק כוונת המשורר?

מאת: חנית שורצ'ף, MBA - בנק הפועלים

כתיבת דוחות ביקורת - חלק בלתי נפרד מעבודתנו כמבקרים פנימיים.

תקן 2400 מתוך התקנים המקצועיים הבינלאומיים של לשכת המבקרים הפנימיים העולמית (IIA): "מבקרים פנימיים חייבים לדווח על תוצאות מטלת הביקורת".

ואכן, למבקר פנימי נדרשות תכונות רבות (עליו להיות בקיא, מעודכן, בעל יכולות אבחון, ראייה רחבה, דיוק, התעמקות בפרטים, בעל אינטליגנציה רגשית, יכולת הקשבה והסקת מסקנות ועוד...), אך חובה שתהיה לו גם יכולת כתיבה שוטפת וברורה והתנסחות רהוטה ומדויקת.

על פי תקן 2420 - "הדיווחים חייבים להיות מדויקים, אובייקטיבים, ברורים, תמציתיים, בונים, שלמים ובמועד".

אין ספק שהמשפט שלעיל נכתב על ידי מבקר!
ומהי בדיוק כוונת המשורר?

מדויקים

"נקודי טעויות ופיזותים ונאמנים למובאות"
(מתוך ההגיאור לתקן).

הצורך לדייק בכתיבה הוא קריטי. הדיווחים צריכים להתבסס על ממצאים חלוטים, מתועדים ומאומתים. אלא שמרוב רצון לדייק אנו נוטים להיזהר במיוחד, ולהוסיף שלייקס על החגורה. דוגמאות:

אם בבדיקת תהליך מסוים לא נמצאו ליקויים, לא נכתוב שהתהליך נבדק ונמצא תקין, אלא נכתוב שלא אותרו ליקויים בתהליך.

או למשל, כאשר נרצה לתאר מה בדקנו בביקורת, נכביר בפרטים על מנת לדייק (מילת המפתח - "לרבות"): "בביקורת נבדק המודל החישובי, לרבות תהליך קליטת הנתונים, תהליך עיבוד הנתונים ופלט המודל. עוד נבדק תיעוד המודל, לרבות קיום נוהל פנימי, מסמך תיעוד המודל, נוהל תפעול המודל".

אובייקטיביים

"דיווחים המבוססים, ללא משוא פנים ובלתי מוטים, והינם תוצאה של הערכה שקולה והמונעת של הסובייקטיביות והנסיבות".

אובייקטיביות נמצאת בבסיס תפקידו של המבקר. ככל שקיים חשש לפגיעה באובייקטיביות או באי תלות המבקר, חזקה עליו שיתריע על כך ויימנע מביצוע מטלת הביקורת.

מנגד, מרוב הרצון העז להיות הוגן והגון, אנחנו משקיעים אנרגיות מרובות בניסיון למצוא ניסוחים קרובים או דומים לאותו ממצא:

"המבוקר חרג מסמכותו"; "המבוקר פעל שלא בהתאם לסמכותו"; "הפעולה בוצעה בסמכות שאינה תואמת".

פתרון נוסף הוא שימוש במילת מפתח אחרת - "לכאורה": "המבוקר חרג לכאורה מסמכותו"; "משאבי הבקרה לכאורה אינם מספקים", ועוד.

ברורים

"קלים להבנה והגיוניים, תוך הימנעות משימוש לא נחוץ בשפה טכנית ומתן כל המידע הנחוץ והרלבנטי".

לא תמיד ברור כיצד לכתוב ברור, ובפרט בדוחות ביקורת שעוסקים בנושאים טכניים ומורכבים במיוחד, כדוגמת המשפט שקראתי לאחרונה: "במסגרת סימולציית מונטה קרלו מוגרלים השינויים בשווי הנכסים, בין היתר, לפי תנועות אדיוסינקרטיות שאינן מתואמות עם הלווים האחרים".

תמציתיים

"לשפר של עניין תוך הימנעות ממתן פירוט לא נחוץ, כפולות ומילולית יתר".

ואמנם, בשנים האחרונות מתמודדים המבקרים הפנימיים יותר ויותר עם הצורך לכתוב בצורה מקוצרת ואפקטיבית. סף הסבלנות של הקורא הממוצע התקצר, ואנשים רגילים לצרוך אינפורמציה תמציתית במהירות ונעזרים בסמארטפונים להתעדכנות זריזה בנעשה.

הקורא הממוצע נכנס לאתר חדשותי, מאתר כותרת מעניינת, מתחתיה כתוב "זמן קריאה 10 דקות" - תגובתו המיידית היא סגירת האפליקציה. בקצב של היום, למי יש 10 דקות להקדיש לקריאת כתבה? וכך הקורא מרפרף לו בין כותרת לכותרת, אולי מתעכב על סרטון כזה או אחר (אבל רק אם ניתן לדלג על הפרסומת לאחר מקסימום 7 שניות). אז מי יטרח לקרוא דוח ביקורת מרובה עמודים?

בונים

"למסיימים ללקות המטלה ולארגון להוביל לשיפורים היכן שנדרש".

ברור, הרי זה מהות תפקידנו. רק מה, אין זהירים מאיתנו. הדוגמה הבולטת היא השימוש המרובה במילת מפתח נוספת בולטת - "ככלל":

- "ככלל, לא נמצאו ליקויים".
- "ככלל, נמצאו ליקויים שאינם חמורים, וניתנים לתיקון במהלך העסקים הרגיל".
- "ככלל, התהליך מבוצע בהתאם לנהלים".
- "הביקורת סבורה כי ככלל, מסמך המדיניות הינו בהלימה לתיאבון הסיכון שהוגדר".

שלמים

"איזון מתסירים מידע מיזון למשתמשים ומוליים את כל המידע המשמעותי והרלבנטי לתמיכה בהמלצות ובמסקנות".

וכאן הקושי הגדול - עד כמה לפרט? מידע משמעותי בעיני אחד נראה שולי בעיני אחר.

לשם כך הומצא הפתרון הגאוני המוכר לכל מבקר פנימי - העברה לנספחים. ופעמים רבות ככל שדוח הביקורת מתקצר, כך עמודי הנספחים מתרבים.

במועד

"מתוזמנים, בהתאם למהותיות הנושא, באופן המאפשר להנהלה לבצע פעולות תיקון הולמות".

הדיווח במועד חשוב לצורך אפקטיביות הביקורת. דיווח שיגיע לאחר זמן רב מדי עלול להיות פחות רלבנטי, לאחר שהסוסים כבר ברחו מהאורווה.

באופן הגיוני, על מנת לקצר זמני טיפול ועריכה, עדיף לכתוב באופן מקוצר וממוקד ככל האפשר. באופן מעשי, על מנת לקצר זמני טיפול ועריכה, דוחות ביקורת נותרים לעיתים ארוכים ומלאים בפרטים, העיקר "לרוץ קדימה".

אז מה המסקנה?

- **להמשיך להשתדל.**
- **להוסיף ולהשקיע בפיתוח יכולות הכתיבה של המבקרים.**
- **לתרגל סימולציות של כתיבת ממצאים בקצרה ובאופן ממוקד.**
- **לעודד את המבקרים לנסח את הממצאים תוך כדי הביקורת - כתיבת הממצא מחדדת את המחשבה, מאפשרת להעמיק ולבדוק היבטים נוספים תוך כדי הביקורת בשטח ומקצרת זמנים בסיומה.**

ולמי שצלח את קריאת הטור עד כה - כל הכבוד! באמת שניסיתי לקצר...

Editor's Note

Sharon Witkowski Tabib
CPA, CIA, CRMA

What went through the mind of a young 34-year old woman, who for five years had led a double life?

On the one hand, pleasant personality, Assistant Manager in an Investments Department, devoted and respected by her clients and superiors and a motherof children. and On the other hand, stealing more than NIS 250 millions from the bank where she worked, causing the terminationof her colleagues and the bank's final collapse! There is no answer to that...

I still remember the urgent call I received one Sunday morning in 2002: "Sharon, get as fast as you can to the Trade Bank with an audit team. A large embezzlement has been discovered. It needs to be investigated".

The first day on which the bank's employees arrived at their work place will always be engraved in my mind. The surprise and the shock on their faces were an evident. They sat around, told us stories about their friend Eti, her acts of kindness and her willingness to help everyone. At this point, they had obviously still not grasped the consequences of her actions. They led me to her work station and showed me, with almost a sense of pride, the certificate she received for outstanding work in entrepreneuring.

Towards noon I could see the truth finally dawned on them. I began to see more and more grim faces as they grasped the size of the storm that hit them. The employees were shocked from what she had done and were anxiousns about their future at the bank.

At midday the employees were told they could go home and that the bank would keep them updated on further developments. We all know the outcome, there was no continuity here - in a few days the bank collapsed!

My conclusion and the message that has been engraved in my mind as of that day: **It can happen anywhere .**

Reviling a serious event of fraud or embezzlement can cause us shock and deep anxiety therefore we, **the internal auditors, must always be sharp and alert to such risks.**

But is it enough?

Do professional skepticism, sharpnessand alertness necessarily enable us to identify the next fraud?

To be honest, not nessecerily. The chance of not identifing a fraudulent event exists, but we must do everything in our power to identify it.

In this bulletin, we focus on tools and techniques which internal auditors might employ in order to stay alert and identify fraudulent financial acts as early as possible. I sincerely hope that implementing internal controls and new methods, along with increasing awareness for the ongoing activities in the organization and paying attention to unusual activities, will mitigat the risk of potential fraud and embezzlement, or at least make it extremely more difficult to carry out.

In conclusion, I wish to quote from Pirkei Avot (Ethics of the Fathers):

"It is not your responsibility to finish the work of perfecting the world, but you are not free to desist from it either."

As an analogy to our business – we the internal auditors may not necessarily discover all frauds and embezzlements acts in the organization, yet we are expected to make any effort to detect them, and we have no right to refrain from doing so.

Best wishes for happy holidays and enjoyable reading,

Sharon Witkowski-Tabib

President's Note

Doron Cohen
CPA, President IIA Israel - Institute of Internal Auditors

From time to time, a substantial fraud is detected in Israel or somewhere around the world, and it immediately brings up the question: “where was the internal auditor?“.

On one hand, it is good that the public regards us, the internal auditors, as having an important role in preventing fraud and embezzlement. However, on the other hand, it also implies that there’s an expections’ gap between the role of internal auditors and their actual level of responsibility.

According to the international standards for the professional practice of internal auditing, internal auditors are expected to have sufficient knowledge to evaluate the risk of fraud, but are not expected to have the expertise of a person whose primary responsibility is to detect and investigate fraud.

The practical implications for the above are that internal auditors must address the risk of fraud when preparing the annual audit plan, on top of various other risks they assess. In addition, when performing an audit engegment, the internal auditor must be conscious of the risk of fraud and drive to improve fraud prevention and detection controls.

Occasionally, as a result of the audit work , cases of fraud and deception might be revealed and then the internal auditor may take part in the fraud investigation. However, it should be emphasized that fraud detection and prevention is not the primary objective of the internal audit and it is unreasonable to expect that an internal audit will detect all frauds with its limited resources.

It is our hope that through the present bulletin, which is dedicated to the prevention and detection of fraud, you will familiarize yourself with the diverse approaches and tools available when confronting this challenging issue.

The IIA Israel has been sucsessful in its efforts to influence the recommendations of an interministerial team, to explore the possibility of setting up a special purpose stock exchane for small and medium-sized companies. The interim report, issued in November 2017, included a recommendation to exempt companies with a certain volume of activity or characteristics from the obligation to appoint an internal auditor. In a position paper published by the IIA on January 2018, it was stated that the internal auditor, as an objective and professional “gatekeeper“, acting as an agent of the board of directors, represents an important line of defense for the organization, irrespective of its size. The IIA position paper argued that the aforementioned directive, would adversely affect investors and shareholders, as well as corporate governance in these companies. Fortunately, the final report published in June 2018 did not include this recommendation.

Recently, IIA Israel published a response to the draft regulation issued by the director of the Government Companies Authority (GCA), regarding internal audit activities withn goverment companies. Although The IIA commended the initiative to strengthen the internal audit in this important sector, it also had reservations regarding some of the recommendations. for instance, the draft regulation does not address the significant matter of assuring sufficent resources for internal audit activities, in order to enable it to function effectively. Furthermore, IIA Israel disagreed with the section of the draft that stipulated that the CEA of companies of a certain size must be a company employee. It is the position of the IIA that the decision about the CEA engagement should be determined by the board of directors.

Wishing you an enjoyable reading,

Doron Cohen

בברכת חג שמח
ושנה טובה!

נשתמע בגיליון הבא

שצפוי לצאת לקראת חג הפסח, תשע"ט

אפריל 2019

Until the next issue, which is expected to be released on april 2019.