



פריצות סייבר ומידע פיננסי לא ציבורי



רועי צוקרמן

ד"ר רועי צוקרמן הוא חוקר בתחום המימון וחבר סגל בכיר בפקולטה לניהול ע"ש קולר באוניברסיטת תל אביב. מחקריו של ד"ר צוקרמן עוסקים בתחום תמחור הנכסים האמפירי ומתמקדים בהשפעה של החדשות והמדיה על תמחור נכסים, קרנות נידור והיבטי סייבר ומימון. ד"ר צוקרמן הוא חבר במכון למחקר סייבר רב-תחומי על שם "בלוטניק" והמחקר האמור נעשה בתמיכה של המכון.

תקציר

במאמר זה אנו בודקים השגה של מידע פיננסי לא-ציבורי באמצעות פריצות סייבר. בעזרת נתונים שנרכשו מספקית ציוד רשת גדולה, אנו מוצאים כי ניסיון לפריצות במשרדי המטה של חברות ציבוריות עולים ב-60% במהלך 14 ימי המסחר שלפני פרסום דוחות רבעוניים. ההתקפות חוזרות לרמות הרגילות מייד לאחר פרסום הדוחות. אנו לא מוצאים אפקט דומה עבור חברות פרטיות במערך הנתונים שלנו. התוצאות נשארות איתנות גם לאחר התאמה ליום בשבוע, לפעילות של תוכנות זדוניות ולהשפעות עונתיות אחרות. אנו מוצאים כי קיים קשר בין פיזור התחזיות של האנליסטים, בין הפתעת הרווח (SUE) ובין פעילות ההאקרים, אולם אנחנו לא מוצאים תשואה חריגה מובהקת עבור החברות במדגם שלנו לפני פרסום הרווחים הרבעוניים. כאשר התוצאות נלקחות יחדיו, הן מרמזות כי להאקרים יש עניין משמעותי בהשגת מידע פיננסי שאינו ציבורי לפני חשיפתו לכלל ציבור המשקיעים.



הקדמה

בתאגידים לצורך ביצוע עסקאות בשוק ההון. בהדלפות הללו היה מעורב מידע שנגע לחלק מחברות הטכנולוגיה הגדולות ביותר הנסחרות, כולל Dell ו-Nvidia, והן הובילו לרווחים לא חוקיים של מאות מיליוני דולרים². דוגמאות אלה כרוכות בהדלפות מצד גורמים בחברה, אולם רבים מהמקרים הנתבעים על ידי ה-SEC כוללים דליפות, לא רק מצד גורמים בחברה, אלא גם מצדדים שלישיים שנחשפים למידע שאינו ציבורי, כגון רואי חשבון, עורכי דין ואפילו חברות יחסי ציבור וחברות הדפסה של חדשות פיננסיות³. עד כה, עיקר תשומת הלב הופנתה למקורות אנושיים של העברת מידע, אבל זו לא בהכרח האפשרות היחידה.

סקנדלים מהשנים האחרונות הדגימו את חשיבות הבעיה של מסחר המתבצע על סמך מידע פנימי בשווקים הפיננסיים. באחת מהשערוריות הבולטות של סחר במידע פנים, ראני ראניארנטנאם, מנהל קרן הגידור Galleon, הורשע בביצוע סדרה של עסקאות בלתי חוקיות על סמך מידע לא פומבי שקיבל מרשת של אנשי עסקים, ובהם ראניט נופטה, לשעבר יו"ר מקינזי, אשר שימש באותה העת כדירקטור בדירקטוריון גולדמן סאקס¹. מקרה מרכזי נוסף קשור לקרן הגידור הנדולה SAC Capital, שבה השתמשו הסוחרים ברשתות מורכבות כדי להעביר מידע לא ציבורי ממקורבים לאנשי פנים

2 ראה www.wsj.com/articles/SB10001424127887324685104578390023688221236

3 ראה www.sec.gov/News/PressRelease/Detail/3PressRelease/1365171484464#VJ1aEV4DA

1 ראה www.wsj.com/articles/SB10001424052970203914304576627191081876286

שנועדו להשיג מספרי כרטיס אשראי או מידע אישי אחר, פריצות שנועדו להשיג מידע פיננסי שאינו ציבורי עלולות לגרום נזק לא פחות משמעותי, אולם הנראות וטביעת הרגל התקשורתית של פריצות מהסוג הזה עשויות להיות זניחות וזאת בשל אופי המידע שהושג. יתר על כן, לחברות עשויים להיות תמריצים שלא לחשוף פריצות מסוג זה.

מחקר זה מתמקד בזיהוי ובחשיפת הראיות שלפיהן האקרים שפועלים במרחב הקיברנטי מעוניינים להשיג מידע פיננסי לא-פומבי של חברות נסחרות, טרם פרסומו לציבור. לפי מיטב ידיעתנו, מחקר זה הוא הראשון אשר לוקח על עצמו את האתגר להציג ראיות לכך שהאקרים פועלים באופן שיטתי להשיג מידע לא ציבורי באמצעות פריצות סייבר. ככזה, למחקר זה עשויות להיות השלכות מרחיקות לכת על החברות ועל האמצעים הנדרשים להבטחת מידע פיננסי לא-ציבורי הן בארגון והן על ספקי השירותים המסונפים אליו. בנוסף, למחקר יש גם השלכות הנוגעות לרגולטורים במאמציהם להגן על הגינות ושיקיפות בשווקים הפיננסיים.

סקירה ספרותית

מחקר הנוגע לסחר במידע פנים

מחקר פיננסי העוסק במסחר במידע פנים התמקד עד כה בעיקר בהיבטים משפטיים של מסחר במידע פנים ובניתוח מקרים ספציפיים ותביעות. עם זאת, נמצאו מספר מאמרים אשר מנסים להסתכל על התופעה ככלל מנקודת מבטו של השוק. לדוגמה, (Pareek & Zuckerman 2017) מצאו כי שינויים גדולים במחיר המניה במהלך 30 הדקות האחרונות של המסחר, בטרם פרסום דוח רבעוני, עשויים לחזות את כיוון ההפתעה ברווחי החברה (SUE). תיק מניות אשר כולל את 10% המניות עם הביצועים הטובים ביותר ב-30 הדקות טרם פרסום הדוח הרבעוני בניכוי 10% המניות עם הביצועים הגרועים ביותר באותו פרק זמן, יקנה תשואה עודפת ממוצעת של מעל 2.5% במהלך יום המסחר שאחרי פרסום התוצאות הרבעוניות. החוקרים מייחסים תוצאה זו לדליפה מוקדמת של הדוח הרבעוני. עם זאת, תוצאה זו אינה מחזיקה במסגרות זמן ארוכות יותר (3 שעות ומעלה), דבר המצביע על כך שהמידע מתקבל רק זמן קצר לפני השחרור המתוזמן (Brenner et. al 2014) מצאו גם הם עדויות למסחר באופציות CALL לפני הודעות מיזוג ורכישה. (Pareek & Zuckerman 2014) גם מצאו כי קיימת נטייה בקרב חברות להיות "עברייניות

בעוד שהדלפות אנושיות של מידע לא-ציבורי מציבות אתגר לרשויות אכיפת החוק, דליפות מידע מהמרחב הקיברנטי (cyber space) עשויות להציב אתגר גדול יותר באופן משמעותי. במהלך חודש אוקטובר 2012, חברת RR Donnelley & Sons, המספקת לחברות ציבוריות שירותי "הדפסה פיננסית" הדליפה בטעות את הדוח הרבעוני של חברת נוגל שעות לפני הפרסום המתוכנן על ידי מילוי טיוטה מקוונת באתר EDGAR.⁴ באותה תקופה, התרחשה גם גניבת נתונים מתוחכמת מחברת טארגט⁵ אשר הפגינה את הפוטנציאל הטמון בהדלפות של מידע מהותי באמצעות פריצות סייבר. בעוד שהיעד העיקרי בתקיפה היה ככל הנראה מידע על לקוחות וכרטיסי אשראי, סביר ביותר כי גם מידע לא ציבורי אחר נלקח, כולל מידע פיננסי לא-ציבורי, שעשוי לשמש לפעילות מסחר בלתי חוקית.

יתר על כן, בשנת 2015, הוגש כתב אישום כנגד יותר מ-150 חברים ברשת האקרים אוקראינית, אשר זכתה לכינוי "אמזון של מידע פנים".⁶ הרשת האוקראינית הואשמה בכך שפרצה למערכות ממוחשבות של חברות ציבוריות וגנבה מהן מידע פיננסי לא-ציבורי, לרבות נתוני מכירות של החברות ודוחות כספיים רבעוניים לפני פרסומם לציבור. חברי הרשת לא סחרו במידע בעצמם, אלא מכרו את המידע לכל דורש באמצעות ה-Darknet. הקבוצה נתפסה במבצע עוקץ שנערך על ידי ה-FBI והייתה למקרה המרכזי והראשון שהדגים את הפוטנציאל של פריצה שיטתית המכוונת להשגת מידע פיננסי לא ציבורי ככלל, ודוחות כספיים רבעוניים בפרט.

למרות הראיות המצביעות, לכאורה, על כך שמידע פיננסי מהותי שאינו פומבי עשוי לדלוף באמצעות המרחב הקיברנטי, עד לזמן האחרון נעשו מספר קטן בלבד של מחקרים במטרה לנסות ולזהות את היקף התופעה ואת מקורות ההדלפות, ולבדוק אם אמצעי האבטחה שנקטו החברות (חברות רואי חשבון, משרדי עורכי דין, מדפיסים פיננסיים, חברות יחסי ציבור וכו') מתאימים למניעת דליפות כאלה. שלא כמו פריצות

www.wired.com/2012/10/google-shares-plunge-as-4-earnings-results-leak-early
www.forbes.com/sites/paularosenblum/2013/12/19/5/data-breach-paints-targets-holiday-weekend-black
www.bloomberg.com/news/articles/2015-08-11/hackers-6-100-million-insider-trading-shop-sold-data-on-demand

חזרתו", כלומר קיימות עדויות לדליפות ברבעונים עוקבים בקרב אותן החברות.

מחקר העוסק באבטחת סייבר והשווקים הפיננסיים

מחקרים בנושאים הקשורים לסייבר ולשווקים פיננסיים התמקדו במידה רבה בהשלכות של תקיפות סייבר. מחקרים אלה מתועדים בדרך כלל בתגובות שוק שליליות לאירועי סייבר (Garg et al. 2003; Hinz et al. 2015; Gatzlaff and McCullough 2010; Cavusoglu et al. 2004; Zafar et al. 2016). מוצאים כי לאחר אירוע סייבר, פירמות שיש להן מנהל מידע ראשי (CIO) בצוות ההנהלה הבכירה, מפנינות ביצועים טובים יותר מאלו שאין להן כזה. בספרות הביקורת, Li et al. (2016) מוצאים כי עלויות הביקורת גדלות בעקבות תקיפות סייבר. Westland (2018) מוצא כי פריצות סייבר קשורות באופן ברור לעוצמת הבקרה הפנימית שנבדקה בביקורת הנובעת מחוק Sarbanes-Oxley.

המחקר שלנו קשור גם ל-Gordon et al. (2010) אשר בוחנים את הקשר בין שווי השוק לגילוי מרצון של הסיכון הקיברנטי בין השנים 2000 ו-2004. תקופת המדגם שלהם קודמת לדרישות של ה-SEC לדיווח חובה אודות הסיכונים (דרישות משנת 2005) ולהנחיות המשלימות משנת 2011 בנושא גילויי אבטחה ברשת. (Jonah et al. 2018) גורסים כי שבעת הגילויים שבמשטר דיווח החובה הנוכחי מעידים על המחויבות של חברות להתמודד עם סיכוני סייבר, ומוצאים כי שווי השוק של החברות המנלות גבוה יותר. (Gordon et al. 2010) מתמקדים בנוכחות או בהיעדר גילויי סייבר, (Jonah et al. 2018) בונים מדד מתמשך המביא לידי ביטוי רחב יותר למודעות cybersecurity באמצעות שימוש במילון מקיף וניתוח טקסטואלי של דוחות K10, על ידי זיהוי אורך הגילויים הרלוונטיים והרלוונטיות של השפה בשימוש (Berkman et al. 2018b).

תקנות SEC על גילויי Cybersecurity

בשנת 2005, בתקופה שלאחר תקופת המדגם של (Gordon et al. 2010), הגילויים לפי סעיף 1A הפכו למנדטוריים באמצעות תקנה (SEC) S-K Item 503(c) (2005), לפיה חברות נדרשות לחשוף ולתאר גורמי סיכון ספציפיים לחברה. בעוד שחברות נדרשות לחשוף את כל הסיכונים המהותיים, הנחיות אלו לא התייחסו במפורש לגילוי הסיכונים והאירועים בתחום הסייבר (SEC 2011). במאמץ

לספק שקיפות מוגברת בנושאים הקשורים לאינטרנט, ה-SEC פרסמה בשנת 2011 הנחיות גילוי CF Disclosure Guidance: Topic No. 2 Cybersecurity (SEC 2011). ההנחיה הדגישה כי על חברות החשופות לסיכונים מהותיים הקשורים לסייבר יש חובה לחשוף מידע בנוגע לנושאים מהותיים בתחום ה-cybersecurity (SEC 2011).

התחומים העיקריים בדוח ה-10K (הגילוי השנתי) שבהם נדרשות החברות לספק גילוי של סיכונים והזדמנויות הקשורים לביטחון הקיברנטי כוללים את הדיון של ההנהלה וניתוח המצב הכספי ותוצאות הפעילות (MD&A), תיאור העסק, תיאור ההליכים המשפטיים, ובסעיף 1A, גורמי סיכון. ההנחיה מצביעה על כך שחברות צריכות לחשוף את הגורמים המשמעותיים ביותר הקשורים לסיכון בהשקעה בחברה (SEC 2011). ה-SEC מזכירה לחברות להימנע גילויים גנריים וכלליים, אלא כדי לספק גילויים נאותים המותאמים לנסיבות שלהם, כך שמשמשים יוכלו להעריך את אופי הסיכונים של החברה.

חשוב לציין כי מנהלים הם אסטרטגיים בהתנהגות הגילוי שלהם (Dye 1985; Jorgensen and Kirschenheiter 2003). אם לחברות יש סיכונים ספציפיים בסייבר, חשיפת מידע רב מדי או ספציפי מדי לגבי הסיכונים עלולה להפוך את החברה לפגיעה יותר להתקפות (Rogers and Van Buskirk 2009), למרות שגילוי מוגבר עשוי להפחית את סיכון ההתדיינות המשפטית (Francis et al. 1994; Gordon et al. 2010). לפיכך, בעת זיהוי הסיכונים המהותיים, ההנהלה יכולה לדון בקצרה ובאופן מעורפל בתחומים של חולשה. לדוגמה, מנהלים יכולים להימנע מלספק מידע כמותי על הסיכונים שלהם על ידי שימוש בשפה דו-משמעית שאינה מספקת מידע נוסף (Dye 2010), או שהם יכולים למקד את הדיון שלהם בסיכונים מהותיים שהחברות כבר מטפלות בהם. האופי האיכותי של גילויים בסיכון מקל על מנהלים להיות אסטרטגיים בגילויים שלהם. לנוכח הסיכונים המשמעותיים הקשורים לגילוי של פגיעויות, ניתן לראות בגילויים הקשורים בסייבר כמשקפים את רמת המודעות של החברה לנושאים העוסקים ב-cybersecurity.

מעבר לגילויי החשיפה הכלליים שיוגשו במסגרת דוח ה-10K של החברה, תקנות ה-SEC קובעות שחברות גילו כל תקיפת סייבר מהותית במהירות האפשרית (כלומר בדוח מיידי). כלל המהותיות קובע כי אירוע מהותי הוא אירוע שגרם לנזק מהותי

(נהוג לפרש נזק מהותי ככזה שעולה על 2% מההון העצמי של החברה). במקרה שהנזק מהאירוע לא מגיע לסף המהותיות, שיקול הדעת הוא של החברה לשפוט האם האירוע הוא מהותי, ובהתאם להוציא דוח מידי המנלה את האירוע. Amir et al. (2018) מנתחים גילויים של התקפות סייבר ומוצאים שחברות נוטות לחשוף התקפות קטנות ולהסתיר התקפות גדולות. הם גם מראים כי במקרים שבהם חברות לא חשפו התקפת סייבר גדולה, ההתקפה דווחה לאחר מכן על ידי צד שלישי, והחברה עצמה סבלה מתשואה שלילית חריגה של עד 250 נקודות בסיס במהלך 90 הימים שלאחר הגילוי.

מעבר לתקנות ה-SEC, מספר מדינות בארצות הברית (לדוגמה, קליפורניה, מדינת ניו יורק ועוד) קובעות שחברות חייבות לחשוף כל התקפת סייבר שבה נתונים של לקוחות (כגון מספרי כרטיסי אשראי, סיסמאות וכד') נגנבו. גילוי של התקפה כזו חייב להיות מהיר ובמקרים רבים מגובה דוח מידי (K8). בניתוח שלנו של הדיווחים השוטפים (K8) שדווחו על ידי חברות ציבוריות מינואר 2000 עד דצמבר 2017, **לא הצלחנו למצוא ולו דוח יחיד** שבו חברה חשפה כי הדוחות הכספיים או נתונים פיננסיים אחרים שאינם ציבוריים, נגנבו באמצעות התקפת סייבר לפני השחרור הציבורי שלהם. חוסר גילוי זה מגיע למרות העובדה כי קיים מידע ברור המצביע על קיומם של אירועים מסוג זה (לדוגמה החשיפה של הרשת האוקראינית).

השערות המחקר

ההשערה העיקרית שלנו היא כי האקרים משיגים (או לפחות מנסים להשיג) מידע פיננסי שאינו ציבורי באמצעות התקפות סייבר, וזאת לפני הפרסום הציבורי של מידע זה. השערה זו נתמכת, בין היתר, על ידי התביעה של רשת האקרים האוקראינית ("אמזון של סחר במידע פנים") במהלך שנת 2015. רשת זו פרצה, לכאורה באמצעות מרחב הסייבר, לחברות ציבוריות ונגבה מידע הנוגע לדוחות כספיים לפני הפרסום הציבורי שלהם. כפי שצוין לעיל, התקנות הפדרליות הנוכחיות אינן דורשות במפורש כי פירמות יחשפו אירועים שבהן הדוחות הכספיים שלהן נגנבו, באמצעות תקיפת סייבר, לפני השחרור שלהם לציבור, שכן אירוע שכזה אינו עונה בהכרח על כלל המהותיות. בהתאם, איננו מכירים ולו מקרה יחיד של חברה ציבורית אשר גילתה כי הדוחות הכספיים שלה נגנבו טרם פרסומם, וזאת אף על העובדה כי התביעה של הרשת האוקראינית מספקת ראיות כי פעילות שכזו אכן התרחשה. אנו מציעים לבחון את ההשערה כי האקרים קיברנטיים מעוניינים במיוחד בהשגת מידע פיננסי לא ציבורי בטרם

פרסומו על ידי נתוני Firewall, וכן לבדוק אם מספר ההתקפות גדל לפני תאריך השחרור. מאחר שהנתונים הנוגעים להרכבת הדוחות הכספיים נאספים ברובם בשבועות המובילים לפרסום הדוח, אנו מאמינים כי אם האקרים מעוניינים בדוחות כספיים רבעוניים, אז נתוני ה-Firewall עשויים להראות פעילות פריצה מוגברת לפני פרסום הדוח הרבעוני הרשמי.

בנוסף, אנו מציעים לבחון את המתאם בין נתוני ה-Firewall, תשואות המניות המותאמות לסיכון ומאפייני החברה כדי לבחון אם פעילות הפריצה מתבטאת גם בהשפעה על מחירי המניות ואם האקרים בוחרים להתמקד בחברות בעלות מאפיינים ספציפיים. אנו מצפים למצוא כי האקרים המעוניינים בדוחות הכספיים יתמקדו בחברות אשר יש להן הפתעת רווח משמעותית באופן היסטורי ופיזור גבוה יותר בקרב הערכות האנליסטים, שכן אלה עשויים לשאת את הפוטנציאל לרווחים גבוהים יותר ממסחר על סמך נתונים שאינם ציבוריים.

יתר על כן, אנו משערים כי פירמות קטנות ובינוניות עשויות להיות אטרקטיביות יותר להאקרים, מאחר שהן צפויות להשקיע פחות בהגנת סייבר בכלל, ובהגנה על הנתונים הפיננסיים בפרט. מצד שני, ייתכן כי דווקא חברות גדולות יהיו מטרות, בשל רמת הניזלות הגבוהה יותר והאפשרות לבנות פוזיציה משמעותית בלי לגרום לתנודת מחיר משמעותית.

נתונים

הנתונים העיקריים המשמשים במחקר זה הם נתוני Firewall שהתקבלו מחברת חומרה גדולה, אשר פועלת גם כספקית תוכנה. ה-Firewall מתעד כל ניסיון לתקוף את הרשת ומסווג כל ניסיון תקיפה על פי החומרה. התוכנה תתעד את האתר המותקף ואת חותמת הזמן המדויקת שבה זוהתה התקיפה לראשונה. הנתונים שלנו כוללים למעלה ממיליון ניסיונות תקיפה באתרים ספציפיים של חברות פרטיות וציבוריות, אשר בהן מותקנת מערכת ה-Firewall של הספק.

תקופת איסוף הנתונים היא בין ינואר 2010 לדצמבר 2015. המדגם כולל 16,283 חברות פרטיות ו-93 חברות ציבוריות. הנתונים מאוגדים לפי יום המסחר (יום המסחר). אנו משתמשים בנתונים אלה כדי לבנות סדרת זמן (time series) של תקיפות סייבר סביב דוחות רבעוניים. כמו כן, אנו ממוזגים נתונים אלה עם נתוני CRSP COMPUSTAT הסטנדרטיים כדי לבחון את המתאם בין נתוני ה-Firewall לבין תשואות המניות ומאפייני החברות המותקפות.

מתודולוגית המחקר

הניתוח הראשוני של הנתונים מתבצע על פי נתוני ה-Firewall. ננסה לבדוק האם נתוני ה-Firewall מראים פעילות תקיפה מוגברת בתקופה שמובילה להודעת הרווחים (יום 0). הניתוח נעשה באמצעות מתודולוגיות שונות, החל מהשוואה פשוטה ועד למודל רגרסיה המודד רציפות. כדי לוודא שהממצאים אכן נכונים, נציג תוצאות עבור מספר מודלים מתאימים.

שאר הניתוח יבוצע באמצעות רגרסיות סטנדרטיות המשמשות בספרות הפיננסית. במסגרת מבחני התשוואה שלנו, ננסה למצוא את המתאם בין פעילות ה-Firewall לבין התשואות בתקופות שלפני ואחרי שחרור הדוחות הרבעוניים. לשם כך נשתמש ברגרסיה מסוג OLS בצורה הבאה:

$$ABS(ABRet(-14,0)) = \alpha + \beta_1 \Delta Attacks_{it} + \beta_2 Controls_{it} + \varepsilon_i \quad (1)$$

$$ABS(ABRet(0,1)) = \alpha + \beta_1 \Delta Attacks_{it} + \beta_2 Controls_{it} + \varepsilon_i \quad (2)$$

כאשר זו התשוואה העודפת (בערכה המוחלט ומותאמת לסיכון על פי מודל DGTW) לתקופה הרלוונטית, $\Delta Attacks_{it}$ היא העלייה (ירידה) ברמת פעילות הפריצה הנגזרת מנתוני ה-Firewall בימים (-14,0).

תמצית התוצאות

תרשים 1 מציג תוצאות מהניתוח של נתוני ה-Firewall. כפי שניתן לראות בתרשים, קיימת עלייה משמעותית של עד 60% במספר ההתקפות על חברות ציבוריות לפני שחרור דוח הרווחים הרבעוני (מספר התקיפות הממוצע² לכל אתר מנורמל ל-100% ברמה שנתית). העלייה בניסיונות הפריצה מתחילה סביב 14 ימי מסחר לפני פרסום הרווחים (יום מינוס 14) וגדלה באופן די מונוטוני עד יום השחרור עצמו (יום 0), ואז יורדת יום אחרי. אנחנו לא רואים את אותו אפקט בקבוצת הבקרה של החברה הפרטית שלנו. התוצאות מחזיקות גם כאשר אנו משתמשים בסדרה של controls, הכוללת יום בשבוע, אירועי סייבר גדולים, את מאפייני החברות ועוד.

ניתוח של מודל הרגרסיה הלא רציפה (regression discontinuity model) מראה כי העלייה במספר ניסיונות הפריצה ב-14 יום הקודמים לפרסום הדוחות הכספיים ועד

7 הניתוח נעשה בעזרת נרמול למספר ההתקפות החציוני לשנה (להבדיל ממספר ההתקפות הממוצע). התוצאות המוצגות בתרשים 1 דומות מאוד באופן איכותי לתוצאות המנורמלות למספר ההתקפות החציוני.

ליום הפרסום עצמו, שונה מהותית משאר הימים במדגם וזאת ברמת מובהקות של 1%. לצורך הגילוי הנאות, יש לציין כי אנו מתעדים אך ורק ניסיונות פריצה. איננו יודעים אם הפריצה הצליחה או איזה מידע נגבב אם בכלל. אולם, לדעתנו, העלייה המובהקת במספר ניסיונות הפריצה מעידה באופן ברור על כך שהאקרים קיברנטיים מתעניינים במידע פיננסי לא ציבורי ופועלים לגנוב מידע זה בטרם הוא מתפרסם.

טבלה 1 מציגה את תמצית המאפיינים של ניסיונות הפריצה. לא מצאנו קשר בין גודל החברות לבין העלייה במספר ניסיונות הפריצה, ולא נראה שחברות גדולות או קטנות סובלות יותר מתופעה זו. לא מצאנו גם קשר מובהק בין יחס של שווי שוק לשווי בספר (Market-to-Book) לבין העלייה במספר ניסיונות הפריצה לפני פרסום הדוחות הכספיים או לתשואות קודמות של אותן החברות. מצד שני, כן מצאנו קשר בין סטיית התקן של ההפתעה ברווחי החברות (SUE) ובין הפיזור בתחזיות האנליסטים (Analyst Forecast Dispersion) לבין מספר ניסיונות הפריצה. כמו כן מצאנו קשר בין סטיית התקן של התשואות של החברות בימים שלאחר פרסום הדוח הרבעוני לבין העלייה במספר ניסיונות הפריצה ברמת מובהקות של 5%. אין זה מפתיע שהאקרים יתעניינו יותר בחברות אשר פוטנציאל ההפתעה בדוח הרבעוני שלהן גדול יותר, ואשר סטיית התקן של התשואות בימים שלאחר הדוח גדולה יותר. כמובן שמשנתנים אלה מתואמים באופן גבוה.

מעבר לעלייה במספר ניסיונות הפריצה, איננו מצליחים למצוא קשר מובהק בין הפריצות לבין תשואות החברות בשוק, כפי שניתן לראות בטבלה 2. כלומר, חברות אשר מצאנו כי יש לגביהן עלייה גבוהה יותר במספר ניסיונות הפריצה אינן מציגות תשואות גבוהות או נמוכות יותר באופן מובהק במהלך התקופה הקודמת לפרסום הדוח הרבעוני. כמו כן איננו מוצאים קשר מובהק בין התשוואה ביום שלאחר פרסום הדוח לבין התשוואה בימים שלפניו (מעבר למה שכבר תועד בספרות). ניתן להסביר את זה בכך שגם במידה שאכן הדוחות נגנבו לפני הפרסום הרשמי שלהם, אין לצפות כי המסחר על בסיס מידע זה יהיה משמעותי מבחינת נפחו וישפיע על המחירים בשוק, בייחוד אם המידע נגבב זמן לא קצר (14 יום) לפני פרסומו. אין לצפות שסוחר מתוחכם ישפיע באופן מהותי על מחירי השוק כאשר יש בידיו זמן לא מבוטל כדי לבנות את הפוזיציה שלו, כל עוד זו קטנה ביחס לשווי השוק ולרמת הניזילות של החברה. כמו כן, איננו מצליחים למצוא

קשר מובהק בין העלייה בניסיונות הפריצה טרם פרסום הדוח לבין התשואה (בערך מוחלט) ביום שאחרי פרסום הדוח.

סיכום

לסיכום, מכלול הראיות במאמר זה מציג עדויות לכך שאכן האקרים קיברנטיים מתעניינים בהשגת מידע פיננסי לא ציבורי בטרם פרסומו הרשמי.

נתוני ה-Firewall מראים באופן גורף כי ישנה עלייה משמעותית ומובהקת במספר ניסיונות התקיפה של החברות הציבוריות במדגם שלנו בימים הקודמים לפרסום דוח רבעוני. מצד שני, לא הצלחנו למצוא השפעה על מחירי המניות

ולא נראה שגודל החברה, יחס ה-Market-to-book שלה או תשואות קודמות קשורים לעלייה זו. כן מצאנו שיש קשר בין הפיזור בתחזיות האנליסטים וסטיית התקן של הפתעת הרווחים ההיסטורית (SUE) לבין העלייה במספר ניסיונות התקיפה.

משטר הרגולציה הנוכחי אינו מחייב חברות לגלות פריצות סייבר שבהן נגנב מידע פיננסי לא ציבורי. לאור העדויות הנורפות במאמר זה ולאור מקורות נוספים ברור שאירועים אלו קורים בשכיחות לא מבוטלת, ולכן יש פה אתגר לרשויות להתאים של המשטר הרגולטורי לפעילות זו.

royz@tauex.tau.ac.il

ד"ר רועי צוקרמן

רשימת מקורות

- Ahern, K. R*. (2017). Information Networks: Evidence from Illegal Insider Trading Tips, 2015. *Journal of Financial Economics* 125 (2017) 26-47.
- Augustin, P., Brenner, M. (2014). Subrahmanyam, M. G*. Informed Options Trading Prior to M&A Announcements: insider Trading? McGill University and New York University. Unpublished working paper.
- Bebchuk, L., Cohen*, A. and Ferrell, A. (2009). What Matters in Corporate Governance? *Review of Financial Studies*, 22(2), 783-827.
- Campbell, K., Gordon, L., Loeb, M., and Zhou, L. (2003). The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security* 11, 431-448.
- Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce* 9, 69-104.
- Chakravarty, S., McConnell, J.H. (1999). Does Insider Trading Really Move Stock Prices? *Journal of Financial and Quantitative Analysis*, 34, 191-209.
- Chernick, M. (2007). *Bootstrap Methods: A Guide for Practitioners and Researchers*, 2nd Edition. Wiley, New York.
- Cohen, L., Frazzini, A., Malloy, C. (2010). Sell Side School Ties. *Journal of Finance* 65, 1409-1437.
- Ettredge, M., Richardson, V. (2003). Information Transfer Among Internet Firms: the Case of Acker Attacks. *Journal of Information Systems* 17, 71-82.
- Fama, E., and French, K. (1996). The CAPM is Wanted, Dead or Alive. *The Journal of Finance* 51(5), 1947-1958.
- Ge, W., and McVay, S. (2005). The Disclosure of Material Weaknesses in Internal Control after the Sarbanes-Oxley Act. *Accounting Horizons* 19(3), 137-158.
- Gordon, L., Loeb, M., and Zhou, L. (2011). The Impact of Information Security Breaches: Has there been a Downward Shift in Costs? *Journal of Computer Security* 19, 33-56.
- Grossman, S. (1981). The Informational Role of Warranties and Private Disclosure about Product Quality. *Journal of Law and Economics* (December 1981), 461-483.
- Hilary, G., Segal, B., and Zhang, M. (2016). Cyber-Risk Disclosure: Who Cares? Working paper, Georgetown University and Fordham University.
- Hovav, A., D'Arcy, J. (2003). The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review* 6, 97-121.
- Jarrell, G.A., Poulsen, A.B. (1989). Stock Trading before the Announcement of Tender Offers: Insider Trading or Market Anticipation? *Journal of Law, Economics and Organization* 5, 225-248.
- Jung, W., Kwon, Y. (1988). Disclosure when the Market is Unsure of Information Endowment of Managers. *Journal of Accounting Research* 26 (1), 146-153.
- Kannan A., Rees, J., and Shridhar, S. (2007). Market Reactions to Information Security Breach Announcements: An Empirical Analysis. *International Journal of Electronic Commerce* 12, 6991.

Kaszniak, R., and Lev, B. (1995). To Warn or not to Warn: Management Disclosures in the Face of an Earnings Surprise. *Accounting Review*, 113-134.

Kothari, S. P., Shu, S., & Wysocki, P. (2009). Do Managers Withhold Bad News? *Journal of Accounting Research*, 47(1), 241-276.

Kvochko, E., Pant, R. (2015). Why Data Breaches don't Hurt Stock Prices. *Harvard Business Review*, March 31, 2015.

Levitt, A. (1998). The numbers game. *The CPA Journal* 68.12, 14-19.

Securities and Exchange Commission (SEC). (2011). Division of Corporation Finance, CF Disclosure Guidance, Topic No. 2 – Cybersecurity (October).

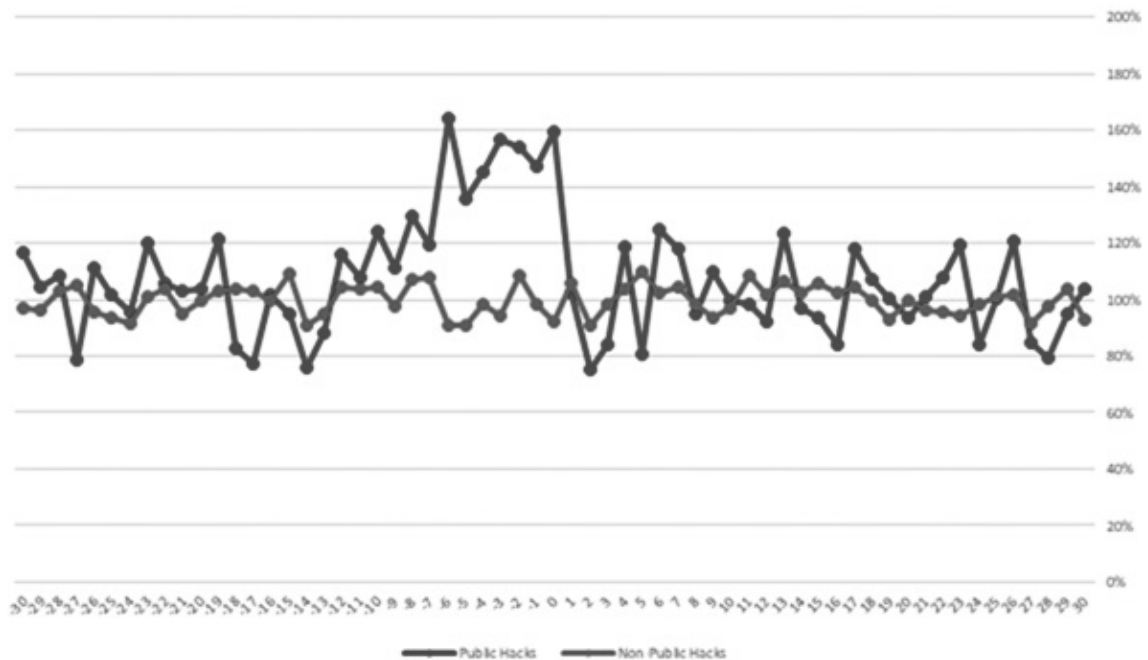
Securities and Exchange Commission. (2013). Enforcement Manual Securities and Exchange Commission. Division of Enforcement. Washington, D.C.

Skinner, D. (1994). Why Firms Voluntarily Disclose Bad News? *Journal of Accounting Research*, 38-60.

Skinner, D. (1997). Earnings Disclosures and Stockholder Lawsuits. *Journal of Accounting and Economics* 23, 249-282.

תרשימים וטבלאות

תרשים 1



תרשים זה מתאר את המגמות בניסיון להתקפות רשת במדגם של 93 חברות ציבוריות ו-16,283 חברות פרטיות. הנתונים מצטברים מדי יום על בסיס ימי מסחר (משעה 16:00 לאחר סיום המסחר ועד שעה 9:29 לפני תחילת המסחר ביום המסחר העוקב). הציר האופקי מציג את יום המסחר, שבו יום אפס הוא היום שבו מתפרסמים הדוחות הרבעוניים. הציר האופקי מראה את הנפח הממוצע של ההתקפות במהלך יום המסחר, כאשר 100% מנורמל לנפח הממוצע השנתי לכל פירמה. הקו האדום מתאר את היקף ההתקפות הממוצע על חברות ציבוריות, ואילו הקו הכחול מתאר את היקף ההתקפות הממוצע על חברות פרטיות.

טבלה 2: התקפות סייבר ותשואות סביב פרסום דוחות כספיים

	Dependent Variable		
	ABS (ABRet(-14,0))		ABS (ABRet(0,1))
	(1)	(2)	(3)
$\Delta Attacks_{it}$	0.501 (1.69)*	0.629 (1.56)	0.744 (1.35)
Log (Size)_{it}	0.312 (0.84)	0.629 (0.78)	-0.519 (-0.95)
MB_{it}	-0.055 (-0.57)	-0.047 (-0.23)	0.027 (0.31)
AnalystDisp_{it}		0.133 (1.14)	0.903 (2.24)**
ABS(SUE)_{it}		0.024 (2.07)**	
R_2	1.12%	1.47%	0.82%

טבלה זו מתארת את הקשר בין התשואה העודפת סביב פרסום הדוחות הכספיים הרבעוניים לבין מספר גורמים. המשתנים התלויים הם התשואה העודפת (בערך מוחלט) ב-14 ימי המסחר טרם פרסום הדוחות הכספיים וביום המסחר הראשון מייד אחרי פרסום הדוחות. המשתנים הבלתי תלויים הינם לוג של שווי השוק (size) (במיליונים), יחס שווי שוק לשווי ספרים (MB), פיזור תחזיות האנליסטים (AnalystDisp) והפתעת הרווח (SUE) בערך מוחלט.

טבלה 1: המאפיינים של התקפות סייבר

	Dependent Variable	
	Attacksit Δ (1)	Attacksit Δ (2)
$Beta_{it}$	-0.131 (-0.26)	-0.072 (-0.17)
Log (Size)_{it}	(3.914) (-0.91)	2.971 (0.75)
MB_{it}	0.015 (0.37)	0.021 (0.52)
ABS(SUE)_{it}		0.107 (2.26)**
R^2	3.75%	9.52%

טבלה זו מתארת את המאפיינים של הגידול (קיטון) בהתקפות סייבר ב-14 הימים טרם פרסום דוחות כספיים רבעוניים. המשתנה התלוי הוא הגידול (קיטון) באחוזים במספר ההתקפות ב-14 ימי המסחר טרם פרסום הדוחות הכספיים. המשתנים הבלתי תלויים הינם הבטא (Beta) של החברה, לוג של שווי השוק (size) (במיליונים), יחס שווי שוק לשווי ספרים (MB), פיזור תחזיות האנליסטים (AnalystDisp) והפתעת הרווח (SUE) בערך מוחלט.