

נזקי המוניטין בעקבות מתקפות סייבר עלולות לגבות מחיר עסקי מחברות

דוח מיוחד | אוקטובר 2020

מידרוג מפרסמת מעת לעת דוחות מיוחדים הנוגעים לענפים או מנפיקים מסוימים. הדוחות המיוחדים אינם מהווים דוחות דירוג ו/או שיטות הערכה מבחינת תכנם או כוונתם ואין בהם כדי לשנות את שיטות ההערכה המתוארות במסגרת הדוחות המתודולוגיים. ככלל, דוחות מיוחדים נועדו על מנת: (1) לפרסם את הערכות מידרוג ביחס לנושאים או להתפתחויות הנוגעות למנפיקים מסוימים, (2) לתאר מגמות מאקרו כלכליות או מגמות בענף ולציין את כיוון השפעתם על הדירוגים (למשל: שינוי בביקושים בענף מסוים, שינויים רגולטוריים לרבות שינויי חקיקה), (3) להסביר תהליכי דירוג מסוימים על מנת לעזור למשקיעים להבין כיצד נקבע הדירוג, לרבות כיצד נלקחות בחשבון בדירוג מגמות מסוימות.

אנשי קשר:

עדי ברנע, אנליסטית

Adi.b@midroog.co.il

סיגל יששכר, סמנכ"ל

ראש תחום מימון תאגידים

i.sigal@midroog.co.il

נזקי המוניטין בעקבות מתקפות סייבר עלולות לגבות מחיר עסקי מחברות¹

הקדמה

סיכוני האשראי עקב אירועי סייבר הולכים וגדלים לאורך השנים, בעיקר בשל הסתמכות הולכת וגוברת על טכנולוגיה בפעילות העסקית. בהתאם לנתוני ה-FBI², מספר אירועי הסייבר עלו בכ-31% וההפסד כתוצאה מהם עלה בכ-238% (מכ-800 מיליון דולר לכ-2.7 מיליארד דולר) בין השנים 2014 ל-2018. בהתאם לממצאי דוח הגנת סייבר לשנת 2019 שפרסם מערך הסייבר הלאומי³, סכום ההשקעה בהגנת סייבר גבוה בענפי המידע והתקשורת והוא עולה ביחס ישיר לגודל החברה ולהימצאות ביטוח כנגד אירועי סייבר.

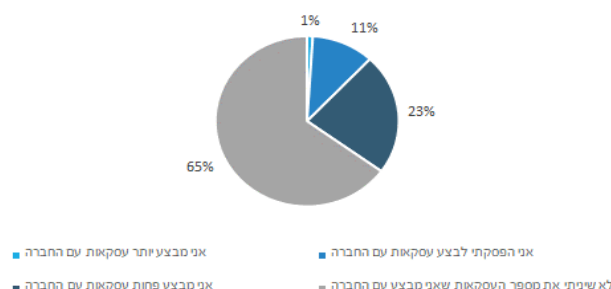
משבר הקורונה הביא לעלייה משמעותית במתקפות סייבר, בעיקר בשל הגדלת השימוש באמצעים דיגיטליים כגון רכישות, תשלומים, ממשק בין חברות לצרכנים ובין חברות לספקים, וכן מעבר לעבודה מרחוק, כל אלו צפויים להגדיל את תקציב הגנת הסייבר בחברות.

בהתאם לסקירת מודי⁴, התקפות הסייבר מעלות את סיכון המוניטין ומציבות דרגות שונות של סיכון אשראי בהתאם לענף הפעילות, גודל החברה והקשר שלה עם לקוחותיה. חברות בעלות עלויות מעבר נמוכות יחסית, כך שלקוחותיהם יכולים להגר בקלות למתחרים, מתבססות באופן משמעותי יותר על קשר של אמון עם הלקוח וחשופות יותר לסיכון מוניטין כתוצאה ממתקפת סייבר על החברה. סיכונים אלו הולכים וגדלים ככל שהתקפות הסייבר נחשפות לציבור, הן מצד המתקיפים כאסטרטגיית סחיטה לתשלום הכופר והן מצד הרגולציה אשר דורשת גילוי מחמיר הדבר אירועי הסייבר בחברות.

התקפות הסייבר מעלות את סיכון המוניטין וההפסד הצפוי בגינו

סוגיית נזקי הסייבר הפכה לסיכון מהותי בפעילות הארגון וליכולתו לעמוד ביעדיו. לצד ההזדמנויות, הטכנולוגיה החדשה מגלמת סיכונים שונים וגדלים, ביניהם, זליגת מידע, דרישות כופר, גניבת כספים ופגיעה בהמשכיות העסקית⁵. התוצאה הברורה ביותר של התקפות הסייבר היא הפסד כספי אשר יכול להיגרם כתוצאה מהונאה, תשלום כופר, קנסות, גידול בעלויות הסייבר, הפסד הכנסות והזדמנויות עסקיות. בהתאם לסקירת EY¹, חברות אמריקאיות הפסידו כ-654 מיליארד דולר בשנת 2019 בשל התקפות סייבר והצפי לשנת 2020 הינו גבוה יותר. בניגוד להשלכות המיידיות של נזקי התקיפה, הכוללות גידול בעלויות ההשקעה בסייבר ואובדן הכנסות מלקוחות ומשקיעים, השלכות הפגיעה במוניטין הינן לטווח ארוך יותר וקשות יותר לאמידה ולכימות. אלו כוללות, בין היתר, אובדן הזדמנויות עסקיות, קושי בגיוס עובדים איכותיים, קושי בגיוס הון ועוד.

חסות צרכנית לחברה לאחר חשיפת מתקפות הסייבר לציבור⁴



¹ סקירה זו מבוססת על נתונים שנאספו מסקירה שערכה מודי¹ "Reputational risks from cyberattacks are rising as episodes become more publicized" מחודש ספטמבר 2020.

² [FBI 2018 Internet Crime Report](#), Internet Crime Complaint Center, April 22, 2019

³ מערך הסייבר הלאומי ומכון המחקר M.I.S - [הגנת סייבר במשק האזרחי בישראל](#), מאי 2019

⁴ MOODY'S - Reputational risks from cyberattacks are rising as episodes become more publicized, 10.09.2020

⁵ בנק ישראל - טכנולוגיה וחדשנות לצד ניהול סיכונים, 20.03.2017

נזקי המוניטין עשויים להבריח את הלקוחות ולפגוע בהכנסות

בשנת 2014 בחברת eBay פורסם כי ארעה דליפת נתונים אשר הובילה לירידה בכמות המשתמשים ובעקבות כך לירידה של כ-200 מיליון דולר בהכנסות החזיות לשנה זו.

בשנת 2015 בחברת אשלי מדיסון התוקפים פרסמו מידע רגיש אודות שמות הלקוחות, שם המשתמש שלהם, סיסמאות מוצפנות ומספרי טלפון, אירוע זה הוביל לירידה בכמות הלקוחות ולירידה של כ-25% בהכנסות החברה.

כמו כן, בשנת 2015 חברת התקשורת הבריטית TalkTalk הפסידה כ-95 אלף לקוחות מתוך 4 מיליון לקוחותיה תוך 3 חודשים בשל דליפת מידע.

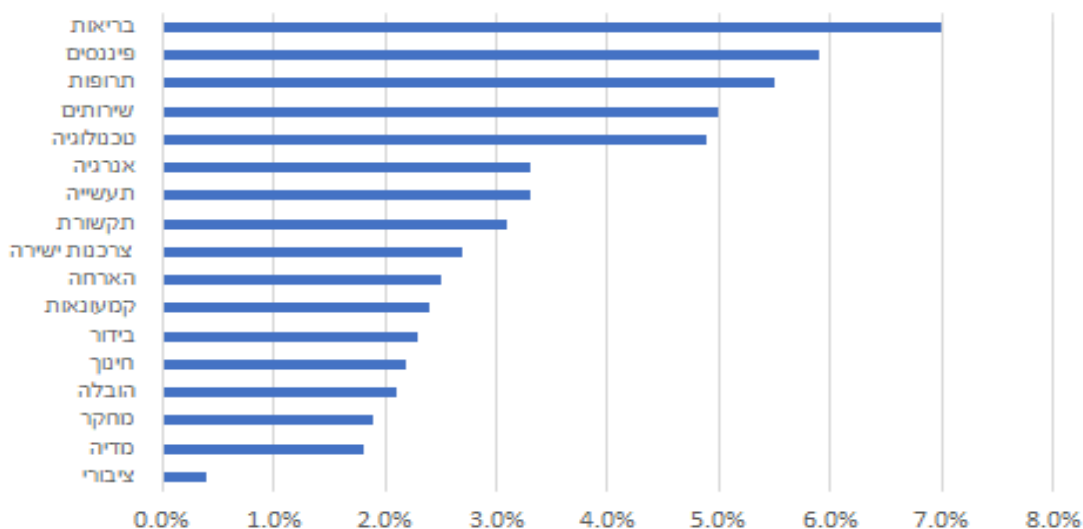
בחודש ספטמבר השנה, פרסמה חברת השבבים Tower Semiconductor כי הפסיקה את פעילות הייצור שלה באופן חלקי לאור מתקפת סייבר. החברה הותקפה בסוג "כופרה", בה האקרים חודרים למערכות הארגון למשך זמן רב וברגע שמאתרים מידע ארגוני בכל ערך נועלים הפורצים את המידע באמצעות הצפנה על מנת לסחוט את הארגון תמורת שחרורו. החברה שבה לפעילות סדורה תוך מספר ימים ופרסמה כי לאירוע זה עשויות להיות השפעות על תוצאותיה ברבעון השלישי לשנת 2020.

בחודש ינואר השנה פרסם בנק דיסקונט כי בעקבות תקלה בהתקנת שרת באפליקציית התשלומים פייבוקס, דלף מידע חלקי של משתמשי פייבוקס. התקלה תוקנה תוך מספר שעות מרגע גילויה. בעקבות אירוע זה הוגשו תביעות ייצוגיות כנגד הבנק בהיקף כולל של כ-1,377 מיליון ₪.

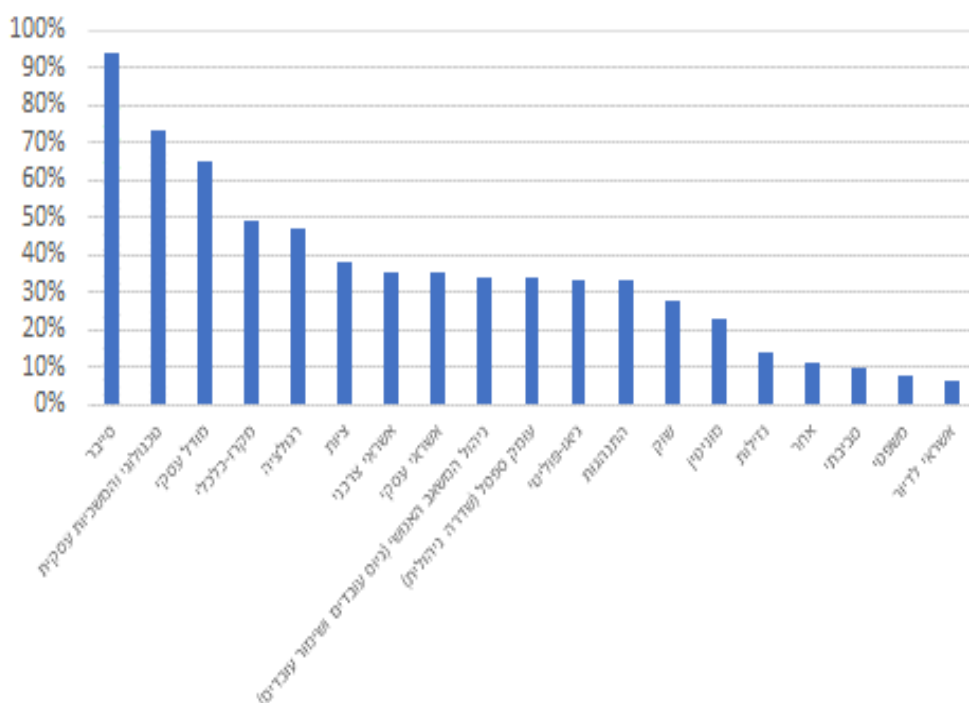
עלויות מעבר נמוכות ורגישות גבוהה לאמון הלקוחות הן בין המאפיינים החושפים חברות לסיכון מוניטין מוגבר כתוצאה ממתקפת סייבר

נזקי המוניטין משתנים בין מגזר למגזר. על פי מחקרה של מודי'ס, הגורמים המרכזיים המשפיעים על סיכון זה הינם כוח המיקוח של הלקוחות ואמון בעלי העניין בחברה. ההשפעה של מתקפת הסייבר עולה ככל שיש ללקוח חלופות רבות יותר כך שיכול לעבור בקלות למתחרים וכן בחברות הכוללות מידע רגיש אודות הלקוח. המגזרים בעלי רמת החשיפה הגבוהה הינם, בין היתר, בנקים, קמעונאות ובראות. זאת לעומת מגזרים בעלי רמת חשיפה נמוכה יותר הכוללים, בין היתר, חברות שירותים, כבישי אגרה, תחבורה ציבורית ושדות תעופה. עם זאת, חברות בעלות ממשל תאגידי חזק עם מדיניות ניהול סיכונים חזקה עשויות להיפגע פחות מסיכון זה.

שיעור עזיבת לקוחות לאחר מתקפת סייבר, לפי ענף פעילות⁴



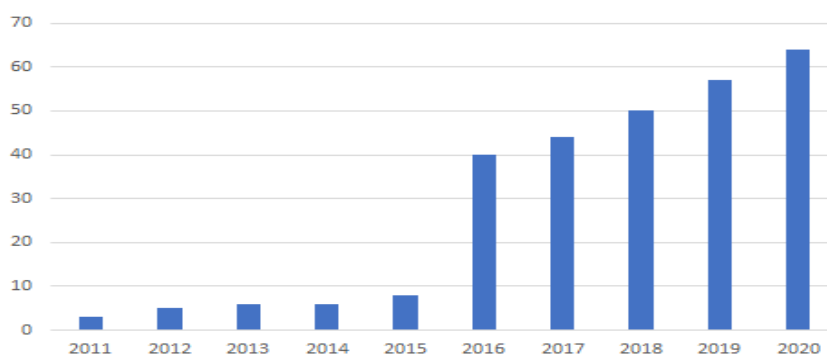
הסיכונים המטרידים את המערכת הבנקאית - סקר הסיכונים של הפיקוח על הבנקים, לשנת 2020⁶



בעבר, חברות רבות התנגדו לחשוף אירועי סייבר מחשש שגילוי כזה עלול להביא להתקפות נוספות ו/או לפגיעה במוניטין שלהן. בשל חובת הדיווח של אירועי סייבר אשר הולכת ומתרחבת במספר רב של מדינות, כאשר בישראל חובת הדיווח הינה חלקית בלבד, החברות נדרשות לקחת בחשבון את אבטחת הסייבר בהחלטותיהן העסקיות. בהתאם לסקירת מודי'ס, מספר ההתקפות המדווחות עלה במחצית הראשונה לשנת 2020 בעיקר בשל משבר הקורונה וכן בשל גידול במספר המדינות המחייבות חברות לדווח כי נפגעו ממתקפת סייבר.

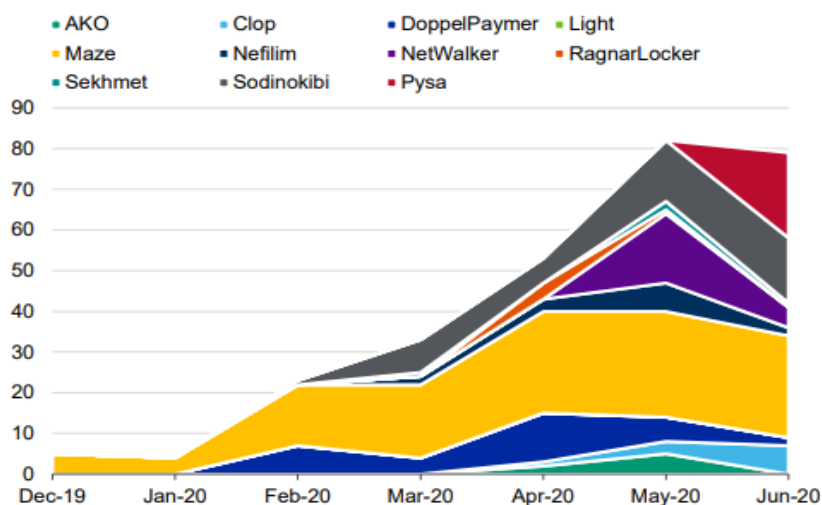
עוד מציינים במודי'ס כי הדרך היעילה ביותר למתן את נזקי המוניטין כתוצאה ממתקפות סייבר הינה באמצעות תגובה מיידית של החברה באופן שקוף ומתן פתרון איכותי לאירוע הסייבר.

מספר המדינות שמחייבות לדווח ללקוחותיהן כי נפגעו ממתקפת סייבר, בין השנים 2011-2020⁴



⁶ [בנק ישראל](#) - התפתחויות וסיכונים במערכת הבנקאות, 06.05.2020

מספר קורבנות ממתקפות סייבר בחודש לפי זהות המתקיפים⁴

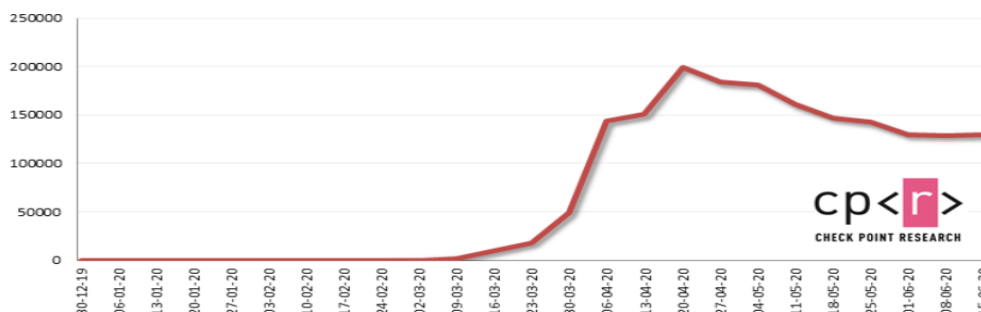


השפעת משבר הקורונה על מתקפות הסייבר

סיכוני האשראי בסייבר הולכים וגדלים לאורך השנים, בעיקר בשל ההסתמכות ההולכת וגוברת על טכנולוגיה בפעילות העסקית, ובהתאם למחקר מברוקינגס⁷ צמיחת הדיגיטציה המהירה ביותר בשנים 2002-2016 הייתה בענפי הבנייה, חקלאות, תחבורה וייצור. בהתאם לנתוני ה-FBI², בין השנים 2014 ל-2018 מספר אירועי הסייבר עלו בכ-31% וההפסד כתוצאה מהם עלה בכ-238% (מכ-800 מיליון דולר לכ-2.7 מיליארד דולר).

ממחקר של חברת Carbon Black⁸, עולה כי משבר הקורונה הביא לעלייה של 238% במתקפות נגד בנקים. בנוסף, החוקרים זיהו כי מתקפות עם אופי פיננסי עולות בסמיכות זמנים לעדכונים חדשתיים חשובים, כדוגמת הדיווח אודות מקרה ההידבקות הראשון בארה"ב או מקרה המוות הראשון במדינה. בהתאם לסקירה EY⁹, 71% מהחברות ציינו כי תמיכה בעבודה מרחוק הינה האתגר הבטיחותי הגדול ביותר. בנוסף, 32% מהחברות שנבחנו צופות כי תקציב להגנת סייבר יעלה וכ-24% צופות כי התקציב יישאר זהה. בהקשר זה, כ-55% מהחברות צופות כי ישקלו לבצע מיקור חוץ של הגנת סייבר לאחר משבר הקורונה.

Weekly Coronavirus Cyber Attacks¹⁰



⁷ [Digitalization and the American Workforce](#), Metropolitan Policy Program at Brookings, November 2017

⁸ מערך הסייבר הלאומי - [סקירה שבועית](#), 17.05.2020

⁹ EY - [COVID-19: How future investment in cybersecurity will be impacted](#), 23.07.2020

¹⁰ [Check Point Blog](#)

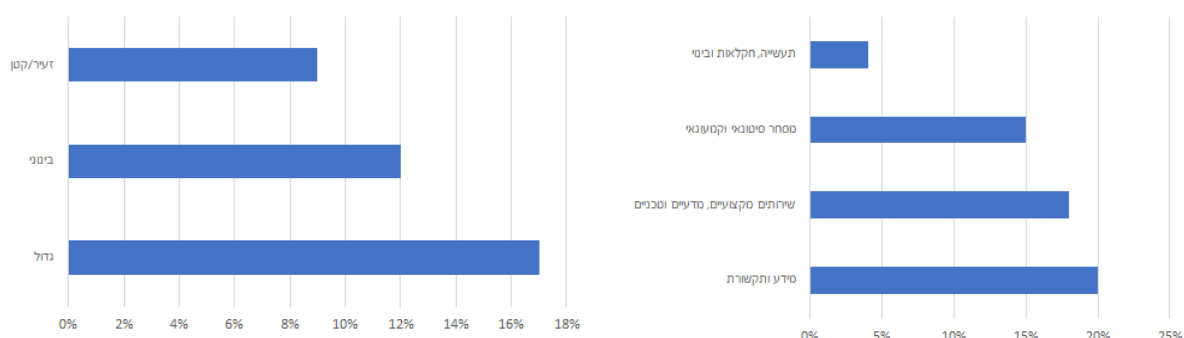
ביטוח כנגד אירועי סייבר

מערך הסייבר הלאומי בישראל³ ערך סקר ובו מצא כי רק ל-13% מהחברות במשק יש ביטוח כנגד אירועי סייבר וכי בכירים רבים בחברות בענפי החקלאות, הבינוי והסיטונות אינם מודעים לכך שקיימת אפשרות לרכוש ביטוח כנגד התקפות סייבר. בנוסף, טענו הנסקרים כי הסיבות העיקריות של החברות להשקעה בביטוח כנגד אירועי סייבר הן ניהול סיכונים, מחויבות ללקוחות ומחויבות למשקיעים. הסיבות העיקריות לבחירה לא להשקיע בביטוח כנגד אירועי סייבר, לעומת זאת, הן חוסר מודעות לאיומי סייבר וחוסר כדאיות כלכלית.

האתגרים המרכזיים בביטוחים כנגד אירועי סייבר הינם תמחור גבוה של הפוליסות וכיסוי שעלול להיות נמוך מגובה הנזק למבוטח, לאור חוסר במידע אקטוארי על הסיכויים להתממשות אירוע סייבר וכן קושי לחזות את פוטנציאל הנזק מהתקיפות. אתגר נוסף הינו היעדר ביקוש, הנובע מכך שהארגונים אינם מודעים מספיק לסיכונים של התקפות סייבר וליתרונות של ביטוח כנגד אירועי סייבר.

מחקר שערך באחרונה מערך הסייבר, שנערך בשיתוף עם לוידיס, העריך את הנזק הכלכלי שצפוי בתרחיש של קטסטרופת סייבר של הדבקה גלובלית על ידי תוכנה זדונית ב־193 מיליארד דולר. ואולם נכון ל־2019, על פי הערכות, חברות הביטוח שפועלות בתחום צפויות לשפות את הנפגעים ב־27 מיליארד דולר בלבד מתוך סכום זה, כך שאת רוב הנזק יאלצו לספוג ארגונים עסקיים ומדינות.

שיעור בעלי ביטוח כנגד אירועי סייבר לפי ענף וגודל חברה³



תאריך הדוח המיוחד: 20.10.2020

© כל הזכויות שמורות לחב' מידרוג בע"מ (להלן: "מידרוג").

מסמך זה לרבות פסקה זו כולל זכויות יוצרים של מידרוג והינו מוגן על ידי זכויות יוצרים ודיני הקניין הרוחני. אין להעתיק מסמך זה או בכל דרך אחרת לסרוק, לשכתב, להפיץ, להעביר, לשכפל, להציג, לתרגם או לשמור אותו לשימוש נוסף למטרה כלשהי, באופן שלם או חלקי, בכל צורה, אופן או בכל אמצעי, ללא הסכמה של מידרוג מראש ובכתב.

אזהרה הנוגעת למגבלות הדירוג ולסיכויי הסתמכות על דירוג וכן אזהרות והסתייגויות בנוגע לפעילות של מידרוג בע"מ ולמידע המופיע באתר האינטרנט שלה

דירוגים ו/או פרסומים שהונפקו על ידי מידרוג הנם או שהם כוללים חוות דעת סובייקטיביות של מידרוג ביחס לסיכון האשראי היחסי העתידי של ישויות, התחייבויות אשראי, חובות ו/או מכשירים פיננסיים דמויי חוב, נכון למועד פרסומם וכל עוד מידרוג לא שינתה את הדירוג או הפסיקה אותו. פרסומי מידרוג יכולים לכלול גם הערכות המבוססות על מודלים כמותיים של סיכויי אשראי וכן חוות דעת נלוות. דירוגי מידרוג ופרסומיה אינם מהווים הצהרה בדבר נכונותן של עובדות במועד הפרסום או בכלל. מידרוג עושה שימוש בסולמות דירוג לשם מתן חוות דעתה בהתאם להגדרות המפורטות בסולם עצמו. הבחירה בסימול כמשקף את דעתה של מידרוג ביחס לסיכון אשראי משקפת אך ורק הערכה יחסית של סיכון זה. הדירוגים שמנפיקה מידרוג הינם לפי סולם מקומי וכאולה הם מהווים חוות דעת ביחס לסיכויי אשראי של מנפיקים וכן של התחייבות פיננסיות בישראל. דירוגים לפי סולם מקומי אינם מיועדים להשוואה בין מדינות אלא מתייחסים לסיכון אשראי יחסי במדינה מסוימת.

מידרוג מגדירה סיכון אשראי כסיכון לפיו ישות עלולה שלא לעמוד בהתחייבויותיה הפיננסיות החוזיות במועד וכן ההפסד הכספי המשוער במקרה של כשל פירעון. דירוגי מידרוג אינם מתייחסים לכל סיכון אחר, כגון סיכון המתייחס לנזילות, לערך השוק, לשינויים בשערי ריבית, לתנודתיות מחירים או לכל גורם אחר המשפיע על שוק ההון.

הדירוגים המונפקים על ידי מידרוג ו/או פרסומיה אינם מהווים המלצה לרכישה, החזקה ו/או מכירה של אגרות חוב ו/או מכשירים פיננסיים אחרים ו/או כל השקעה אחרת ו/או להימנעות מכל אחת מפעולות אלו.

הדירוגים המונפקים על ידי מידרוג ו/או פרסומיה אף אינם מהווים ייעוץ השקעות או ייעוץ פיננסי, וכן אין בהם משום התייחסות להתאמה של השקעה מסוימת למשקיע מסוים. מידרוג מנפיקה דירוגים תחת ההנחה שכל העושה שימוש במידע המפורט בהם ובדירוגים, ינקוט זהירות ראויה ויבצע את ההערכות שלו (בעצמו ו/או באמצעות אנשי מקצוע המוסמכים לכך) בדבר הכדאיות של כל השקעה בכל נכס פיננסי שהוא שוקל לרכוש, להחזיק או למכור. כל משקיע צריך להסתייע ביעוץ מקצועי בקשר עם השקעותיו, עם הדין החל על ענייניו ו/או עם כל עניין מקצועי אחר.

מידרוג איננה מעניקה שום אחריות, מפורשת או משתמעת, ביחס לדיוק, להיותו מתאים למועד מסוים, לשלמותו, לסחירותו או להתאמה לכל מטרה שהיא של כל דירוג או חוות דעת אחרת או מידע שנמסר או נוצר על ידי מידרוג בכל דרך ואופן שהוא.

דירוגי מידרוג ופרסומיה אינם מיועדים לשימוש של משקיעים פרטיים והיה זה בלתי אחראי ובלתי הולם למשקיע פרטי לעשות שימוש בדירוגים של מידרוג או בפרסומיה בקבלתה של החלטת השקעה על ידו. בכל מקרה של ספק, מן הראוי שיתיעץ עם יועץ פיננסי או מקצועי אחר.

כל המידע הכלול בדירוגים של מידרוג ו/או בפרסומיה ואשר עליו היא הסתמכה (להלן: "המידע"), נמסר למידרוג על ידי מקורות מידע (לרבות הישות המדורגת) הנחשבים בעיניה לאמינים. מידרוג איננה אחראית לנכונותו של המידע והוא מובא כפי שהוא נמסר על ידי אותם מקורות מידע. מידרוג נוקטת באמצעים סבירים, למיטב הבנתה, כדי שהמידע יהיה באיכות ובהיקף מספקים וממקורות הנחשבים בעיניה לאמינים לרבות מידע שהתקבל מצדדים שלישיים בלתי תלויים, אם וככל שהדבר מתאים. יחד עם זאת, מידרוג איננה גוף המבצע ביקורת ולכן היא איננה יכולה לאמת או לתקף את המידע. האמור בפרסומיה של מידרוג, למעט כאלה שהוגדרו על ידה במפורש כמתודולוגיות, אינם מהווים חלק ממתודולוגיה על פיה עובדת מידרוג. מידרוג רשאית לסטות מן האמור בכל פרסום כזה, בכל עת.

בכפוף לאמור בכל דין, מידרוג, הדירקטורים שלה, נושאי המשרה שלה, עובדיה ו/או כל מי מטעמה שיהיה מעורב בדירוג, לא יהיו אחראים מכוח הדין כלפי כל אדם ו/או ישות, בגין כל נזק ו/או אובדן ו/או הפסד, כספי או אחר, ישיר, עקיף, מיוחד, תוצאתי או קשור, אשר נגרם באופן כלשהו או בקשר למידע או לדירוג או להליך הדירוג, לרבות בשל אי מתן דירוג, גם אם נמסרה להם או למי מטעמם הודעה מראש בדבר האפשרות להתרחשותו של נזק או אובדן או הפסד כאמור לעיל, לרבות, אך לא רק, בגין: (א) כל אובדן רווחים, בהווה או בעתיד, לרבות אובדן הזדמנויות השקעה אחרות; (ב) כל הפסד ו/או אובדן ו/או נזק שנגרם כתוצאה מהחזקה ו/או רכישה ו/או מכירה של מכשיר פיננסי, בין אם הוא היה נשוא דירוג שהונפק על ידי מידרוג ובין אם לאו; (ג) כל הפסד ו/או אובדן ו/או נזק, אשר נגרמו בקשר לנכס פיננסי מסוים, בין השאר אך לא רק, כתוצאה או בקשר עם רשלנות (להוציא מרמה, פעולה בזדון או כל פעולה אחרת שהדין אינו מתיר לפטור מאחריות בגינה), מצדם של דירקטורים, נושאי משרה, עובדים ו/או כל מי שפועל מטעמה של מידרוג, בין במעשה ובין במחדל.

מידרוג מקיימת מדיניות ונהלים ביחס לעצמאות הדירוג ותהליכי הדירוג.

דירוג שהונפק על ידי מידרוג עשוי להשתנות כתוצאה משינויים במידע שעליו התבסס הדירוג ו/או כתוצאה מקבלת מידע חדש ו/או מכל סיבה אחרת. עדכונים ו/או שינויים בדירוגים מופיעים באתר האינטרנט של מידרוג שכתובתו: <http://www.midroog.co.il>