הארבעה 21 | מגדל פלטינום
תל אביב 6473921
טל. 03-6844700 | פקס. 03-6855002
www.midroog.co.il

סקר סיכוני סייבר בקרב חברות מדורגות

דוח מיוחד | ינואר 2026

מידרוג מפרסמת מעת לעת דוחות מיוחדים הנוגעים לענפים או מנפיקים מסוגים 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 למנפיק/ים מסוימים, 2) לתאר מגמות מאקרו כלכליות או מגמות בענף ולציין את כיוון השפעתם על הדירוגים (למשל: שינוי בביקושים בענף מסוים, שינויים רגולטוריים לרבות שינוי חקיקה), 3) להסביר תהליכי דירוג מסוימים על מנת לעזור למשקיעים להבין כיצד נקבע הדירוג, לרבות כיצד נלקחות בחשבון בדירוג מגמות מסוימות.

אנשי קשר:
ד"ר אביגיל קוניקוב-ליבנה
קצינת אשראי ראשית
avigail.k@midroog.co.il

יואב לייבוביץ
עוזר מחקר מדיניות אשראי
Yoav.L@midroog.co.il

סיכוני סייבר בקרב חברות מדורגות

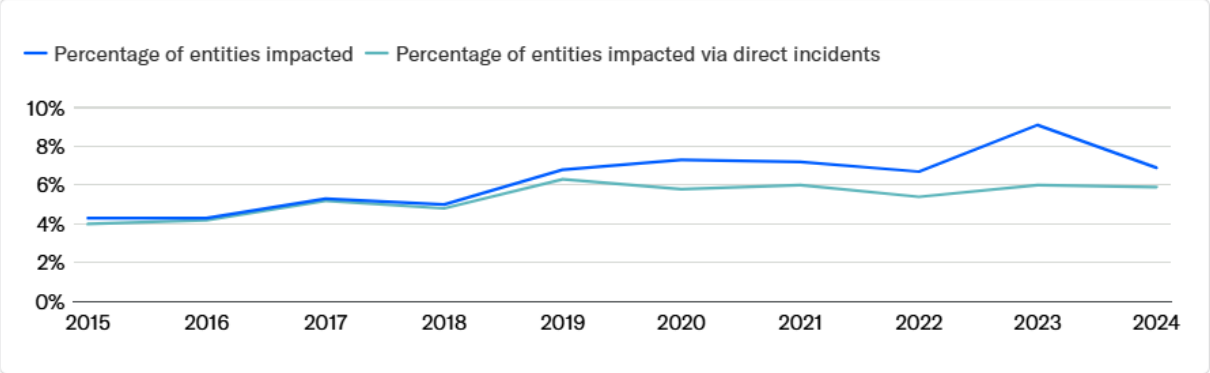
הקדמה

בשנים האחרונות, אירועי סייבר חדלו להיות סוגיה טכנולוגית בלבד והפכו לגורם סיכון המשליך ישירות על הפרופיל הפיננסי ועל התוצאות העסקיות של חברות מנפיקות. לפי נתוני מערך הסייבר הלאומי[1], בשנת 2024 התקבלו כ-17,000 דיווחים על אירועי סייבר,נתון המשקף עליה של כ-24% בהשוואה לכמות הדיווחים שנרשמה בשנת 2023. דוח זה נועד לבחון את החשיפה של מנפיקים מקומיים לסיכונים אלו, תוך הבנה כי אירוע סייבר אינו אירוע נקודתי, אלא אינדיקטור לסיכון מתמשך ולפגיעות מערכתית. בנוסף, הדוח עוסק, בין היתר ברמת המודעות והיקף ההשקעות בתחום הגנת הסייבר בקרב מנפיקי חוב המדורגים על ידי מידרוג, תוך מיפוי וניתוח הפערים הקיימים במוכנות הארגונית וביכולות ההגנה.

השפעות על מנפיקים המדורגים בדירוג גלובלי

ניתוח נתונים גלובלי שבוצע על ידי Moody's[2], המבוסס על מדגם של כ-9,600 מנפיקים מדורגים, מצביע על עלייה עקבית בשכיחות ובתחכום של מתקפות הסייבר. מאז 2020 שיעור המנפיקים שהושפעו מאירועי סייבר מהותיים צמח לכ-7% בממוצע שנתי וזאת בהשוואה לכ-4%-5% בשנה בעשור הקודם.

שיעור המנפיקים שהושפעו מאירועי סייבר בין השנים 2015-2024



*Based on analysis of 9,600 Moody's-rated issuers

Sources: Moody's Ratings, Bitsight Technologies

בהתאם לניתוח ענפי של Moody's ביחס למנפיקים המדורגים בדירוג בינלאומי, נמצא כי קיימת שונות מובהקת ברמת הסיכון בין הסקטורים השונים, הנובעת בעיקר מהשילוב שבין רגישות המידע המוחזק בארגון, לבין איכות תשתיות ההגנה הקיימות. סקטורים המאופיינים במידע בעל ערך גבוה לצד חולשה טכנולוגית או מערכות מיושנות, מציגים חשיפה עודפת לאיומים. דוגמה בולטת לכך היא סקטור **בתי החולים הציבוריים**, אשר הנתונים מלמדים כי מאז שנת 2022, למעלה מ-40% מהמנפיקים בו חוו אירוע סייבר משמעותי. בנוסף, חברה שכבר הותקפה נמצאת בסיכון מוגבר באופן ניכר לחוות מתקפה חוזרת בטווח הקצר, בהשוואה לחברות שלא חוו אירוע כלל. כמו כן, גם **חברות התקשורת** נמנות בין הנפגעות המובילות מאירועי סייבר.

עם זאת, המגמה המסתמנת מצביעה על שינוי באופי האיום: המעבר לתקיפות עקיפות דרך שרשרת האספקה והשימוש הגובר בבינה מלאכותית (AI) על ידי תוקפים, מגבירים את החשיפה של ארגונים, ללא תלות ישירה בחוזק מערכות ההגנה הפנימיות שלהם.

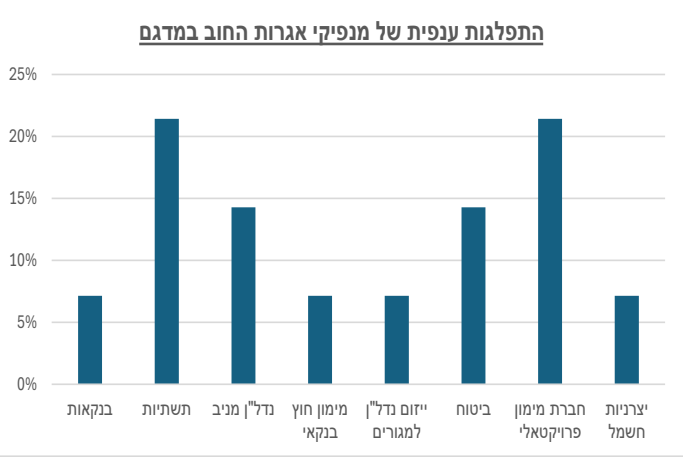
[1] סיכום שנת 2024 - מערך הסייבר הלאומי

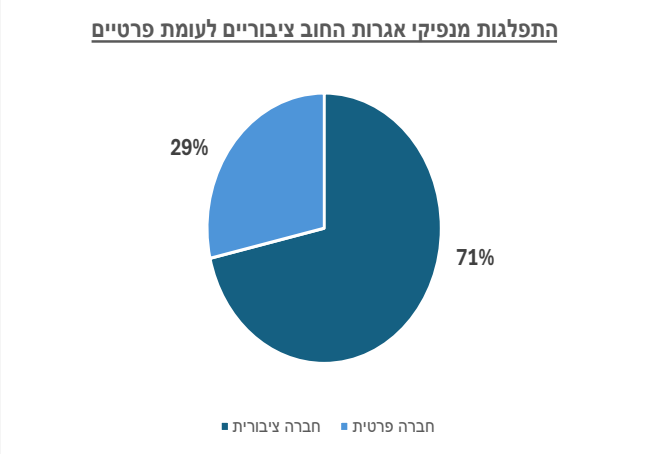
[2] Past cyberattacks are associated with heightened future risks, 10 יוני 2025

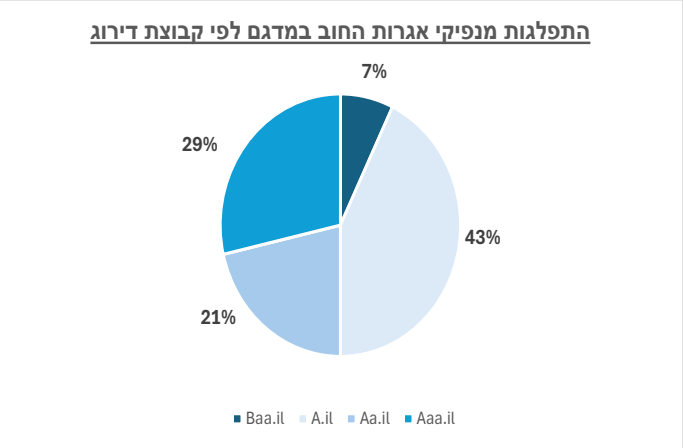
מבחינת דירוג האשראי, ההשפעה הופכת מוחשית יותר - בעוד שעד היום מספר הדירוגים הגלובליים שנפגעו ישירות מאירועי סייבר היה מצומצם, בשנה האחרונה נרשמה עלייה, כולל הורדות דירוג ושינויי אופק, עקב פגיעה תזרימית ושיבושים תפעוליים מתמשכים שנבעו ממתקפות סייבר.

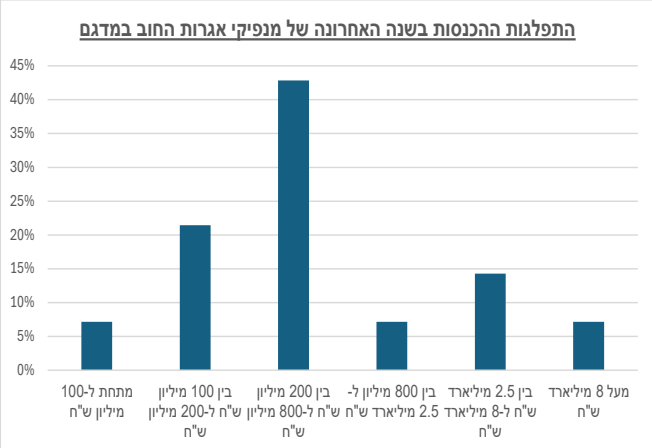
תיאור המדגם

הדוח מתבסס על ניתוח ממצאי סקר שנערך על ידי מידרוג במהלך שנת 2025. הסקר הופץ בקרב אנשי מפתח בכלל החברות המדורגות על ידי מידרוג[3]. המדגם מורכב ממנפיקי אגרות חוב ציבוריים (כ-71% מהמנפיקים במדגם) ופרטיים (כ-29% ממנפיקי אגרות החוב במדגם). במדגם נכללו חברות אשר תחום העיסוק המרכזי שלהן הוא: בנקאות, נדל"ן מניב, ייזום נדל"ן למגורים, חברות מימון פרויקטאלי, יצרניות חשמל, תשתיות, מימון חוץ בנקאי, ביטוח.









בהיבט איכות האשראי, המדגם מורכב ברובו מדירוגי השקעה גבוהים: כמחצית מהחברות (50%) מדורגות בדירוג Aa.il ומעלה. קבוצת הדירוג A.il מהווה את הנתח הגדול ביותר במדגם (כ-43%), בעוד שחברות בדירוג Baa.il מהוות מיעוט של כ-7% מהמדגם.

[3] שיעור ההשתתפות בסקר עמד על כ-7%, נציין כי בשל היקף המדגם, בחלק מהתרשימים תצפיות בודדות עשויות להשפיע באופן מהותי על התפלגות התוצאות.

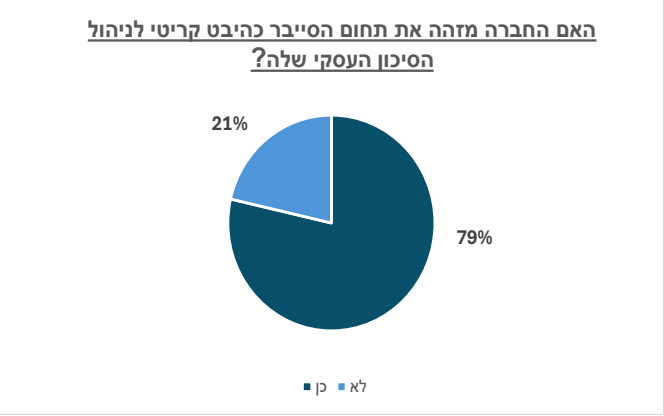
בין החברות הנכללות במדגם קיים פיזור משמעותי במחזורי ההכנסות. "מרכז הכובד" של המדגם נמצא בקרב חברות בסדר גודל בינוני-גדול, כאשר כ-43% מהמנפיקים מציגים מחזור הכנסות שנתי בטווח של 200 עד 800 מיליון ש"ח. לצד זאת, המדגם כולל ייצוג גם לתאגידים גדולים (כ-21% מהחברות עם הכנסות של מעל 2.5 מיליארד ש"ח) וכן לחברות קטנות יותר (כ-28% עם הכנסות של 200 מיליון ₪ ומטה).

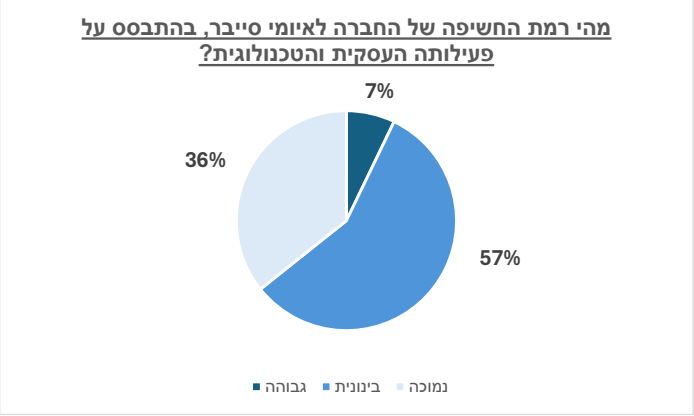
פרופיל החשיפה של המנפיקים לסיכוני סייבר

פרק זה מציג את ממצאי הסקר ביחס לפרופיל החשיפה של החברות המדורגות לאיומי סייבר. הנתונים המוצגים להלן מתמקדים בשלושה היבטים מרכזיים:

- **מידת המודעות והחשיבות שמייחסת ההנהלה לסיכון הסייבר כחלק מניהול הסיכונים הכולל**
- **רמת החשיפה האינהרנטית הנגזרת מאופי הפעילות העסקית והטכנולוגית של החברה**
- **אופן ההתמודדות עם סיכונים הנובעים משרשרת האספקה וגורמי צד שלישי**

להלן תרשימי התפלגות המנפיקים במדגם ביחס למידת החשיבות שמייחסת החברה לסיכוני סייבר ולרמת החשיפה המוערכת שלה כפי שמוגדרת על ידי אנשי מפתח בחברה.

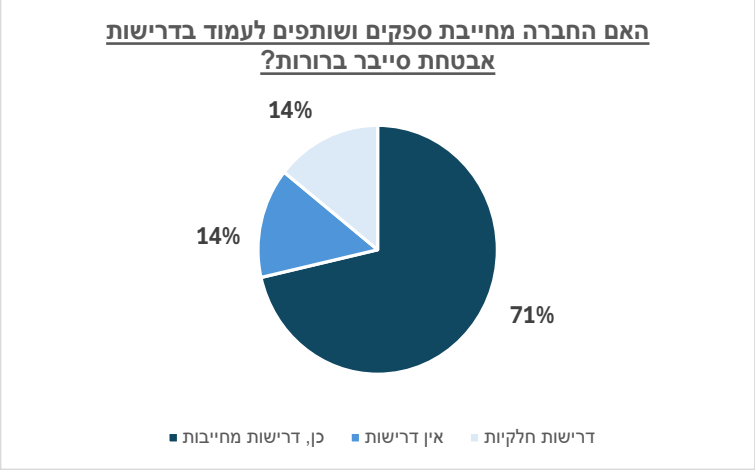




מתוך התרשימים עולה כי עבור מרבית המנפיקים במדגם, סיכוני סייבר מוגדרים כהיבט קריטי המשפיע על ניהול הסיכונים העסקי. עם זאת, בפועל כ-36% מהמנפיקים במדגם אינם מגדירים את עצמם כחשופים במידה משמעותית לאיומי סייבר ורק כ-7% בלבד מהמנפיקים במדגם מגדירים את עצמם כחשופים במידה גבוהה לסיכוני סייבר על בסיס הפעילות העסקית והטכנולוגית של החברה.

בהלימה למגמה הגלובלית, המצביעה על כך שחלק ניכר מנזקי הסייבר מקורו בחולשות אצל גורמי צד שלישי, ניכרת החמרה בדרישות שמציבים המנפיקים לספקיהם ולשותפיהם העסקיים. דרישות אלו נועדו להבטיח יישום מדיניות הגנה נאותה, לצד מזעור החשיפה לסיכונים 'מיובאים'. מגמה זו משתקפת היטב בקרב מנפיקים במדגם, המציגים מודעות גוברת לניהול סיכוני ספקים. עם זאת, באופן גורף, כלל המנפיקים במדגם ציינו כי פגיעות סייבר אצל שותפים או ספקים לא הסבו לחברה נזק ישיר עד כה.

להלן התפלגות המנפיקים במדגם ביחס לרמת דרישות אבטחת המידע המופנות כלפי גורמי צד שלישי:



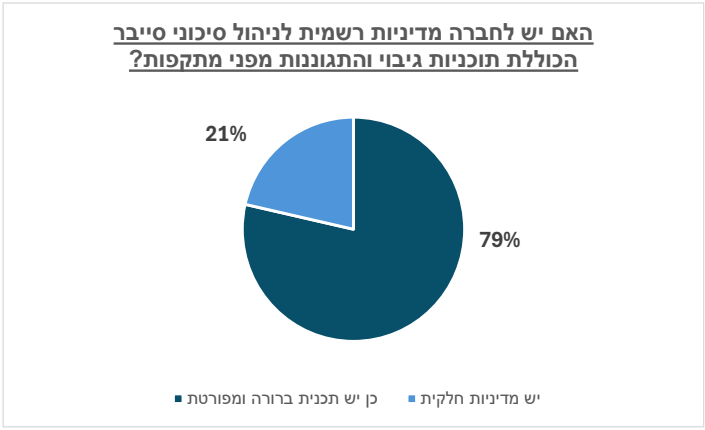
מתרשים זה עולה כי מרבית המנפיקים במדגם מחייבים את ספקי החברה לעמוד בדרישות אבטחת סייבר, אף אם חלקיות. 14% מהמנפיקים אינם משיתים דרישות מסוג זה על ספקי החברה.

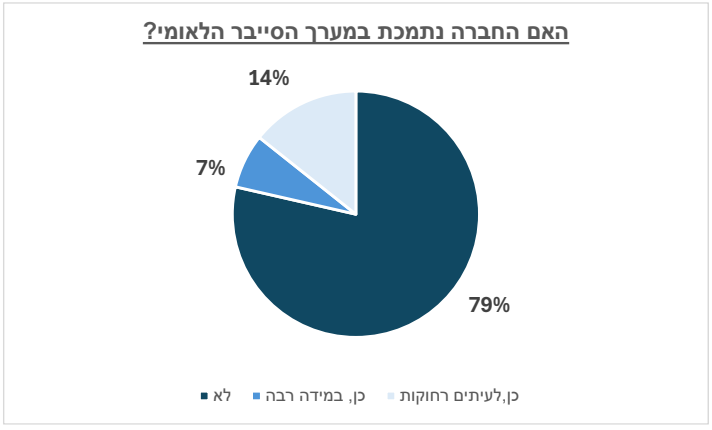
ממשל תאגידי ומוכנות שוטפות

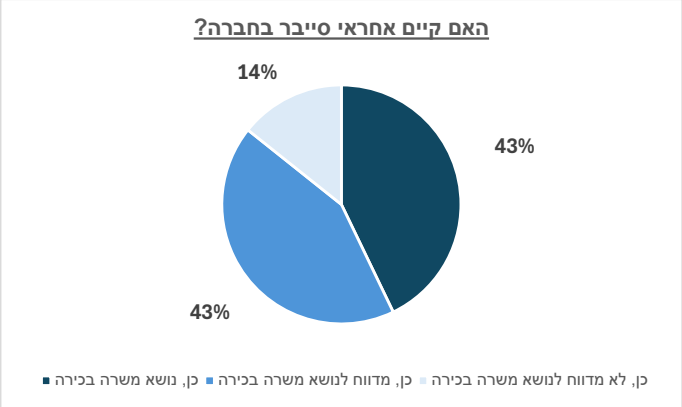
איכות הניהול ומבנה הממשל התאגידי הם גורמים משמעותיים בקביעת פרופיל כושר החזר האשראי של המנפיק. השאלות שנשאלו בסקר הסייבר של מידרוג בנושאים אלו נועדו לבחון היבטים של ממשל תאגידי בקשר עם היערכות המנפיק לאירועי סייבר.

ראשית, נשאלו המנפיקים המשתתפים בסקר בדבר קיומה של מדיניות פורמלית לניהול סיכוני סייבר ותוכניות התאוששות מאסון, המעידות על מעבר מהתנהלות אינטואיטיבית לניהול סיכונים מתודי. שנית, נבחן המבנה הארגוני ומעמדו של מנהל אבטחת המידע בארגון - מתוך ההבנה כי סמכות ועצמאות בניהול האירוע הן קריטיות בזמן אמת. כמו כן, נבדקה מידת ההישענות על מעטפת ההגנה הלאומית (מערך הסייבר), ולבסוף - נבחן החוסן התפעולי, הנמדד במהירות החזרה לשגרה. מדד זה משתקף גם ברמה הכלכלית, שכן התארכות זמן ההשבתה מתרגמת ישירות לפגיעה תזרימית ולשחיקה בכושר שירות החוב.

בתרשימים הבאים מוצגות התשובות שנרשמו בסקר הסייבר של מידרוג בנושאים אלו:







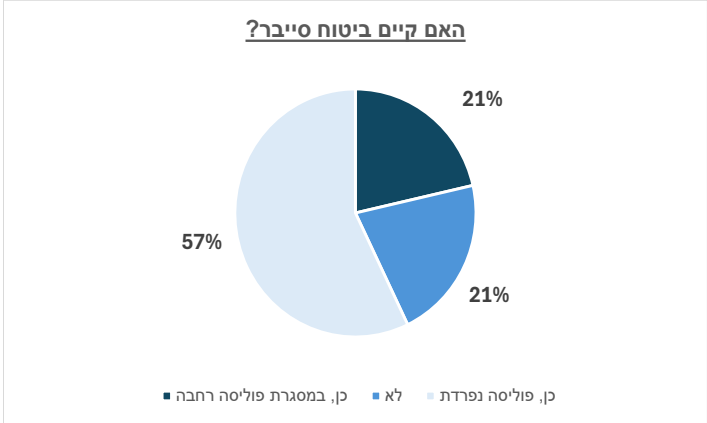
מהתרשימים עולה שכ-79% מהמנפיקים במדגם מחזיקים בתכנית סדורה להתמודדות עם תקיפות סייבר, בעוד לכ-21% יש מדיניות חלקית בלבד. ממצא בולט וחיובי העולה מן הסקר הוא היעדרם המוחלט של מנפיקים החשופים ללא תוכנית התגוננות כלשהי. עם זאת, כלל החברות שדיווחו על קיומה של מדיניות חלקית בלבד, הן דווקא חברות המזהות את הסייבר כהיבט קריטי בניהול הסיכון העסקי. ממצא זה מעיד כי החוסר במדיניות שלמה ומקיפה אינו נובע מהיעדר מודעות לסיכון. הפער נעוץ ככל הנראה באתגרי יישום, במגבלות משאבים או בתהליכי אסדרה פנימיים שטרם הבשילו לכדי מדיניות.

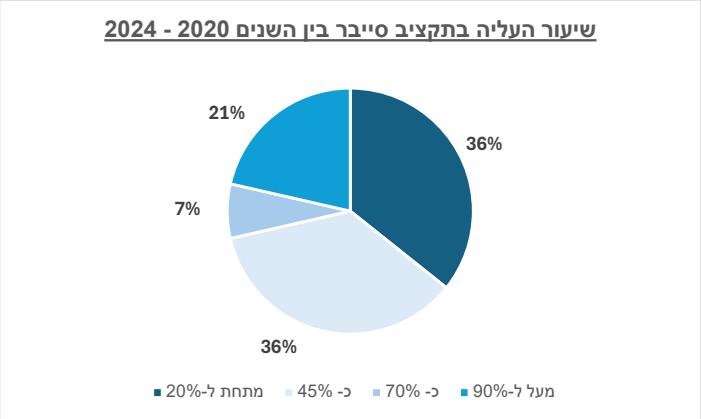
למעט מנפיק אחד, כלל המשיבים על סקר הסייבר של מידרוג מעריכים שייקח להם מספר ימים להתאושש ממתקפת סייבר. המנפיק הנוסף מעריך שמתקפת סייבר על תשתיות פעילות קריטית של החברה תגרור התאוששות של מספר שבועות.

משאבים, השקעות, השפעות פיננסיות וגידור

בחינת נושאים אלו נועדה להעמיק את ההבנה באשר לאופן שבו מנפיקים מתרגמים את החשיפה הגוברת לסיכוני סייבר להקצאת משאבים בפועל ולניהול סיכונים פיננסי. זאת, מתוך תפיסה כי רמת המוכנות הארגונית אינה משתקפת רק במדיניות או בתהליכים פורמליים, אלא גם בהיקף ההשקעה, בהשפעות הכלכליות שכבר התממשו או עשויות להתממש, ובקיומם של מנגנוני גידור וביטוח. שילוב היבטים אלו מאפשר הערכה רחבה ומעמיקה יותר של עמידות המנפיקים בפני אירועי סייבר ושל השלכותיהם האפשריות על פרופיל הסיכון והאיתנות הפיננסית.

להלן מוצגים תרשימים ונתונים אודות היקף ההשקעה וגידור הסיכונים אותם נוקטים המנפיקים במדגם בפועל:





כלל המנפיקים אשר השיבו על סקר הסייבר של מידרוג הצביעו על **עלייה בתקציב הסייבר בין השנים 2020 - 2024**. כ-72% מעידים על עלייה נמוכה מ-50%, עם זאת, כ-21% מדווחים על גידול של יותר מ-90% בתקציב הסייבר שלהם בתקופה זו. שאר המנפיקים במדגם (כ-7%), מצביעים על גידול של כ-70%.

כ־21% מהמנפיקים במדגם אינם מבוטחים בביטוח סיכוני סייבר, לא במסגרת פוליסה רחבה יותר ולא באמצעות פוליסה ייעודית. עם זאת, מן המדגם עולה כי כלל המנפיקים שדיווחו על היעדר כיסוי ביטוחי בתחום זה מגדירים את סיכוני הסייבר כהיבט קריטי בניהול הסיכונים העסקיים שלהם. דיסוננס זה מלמד כי ההחלטה להימנע מביטוח אינה נובעת מהזנחה, אלא משיקולי עלות-תועלת מחושבים בסביבת פרמיות מתייקרת, המובילים את ההנהלות להעדיף השקעה ישירה בחיזוק מערכות המניעה וההגנה על פני העברת הסיכון. משמעות הדבר היא שחברות אלו מאמצות דה-פקטו אסטרטגיה של 'ביטוח עצמי', מתוך הערכה כי חוסנן הפיננסי והטכנולוגי יאפשר להן לספוג ולהכיל אירוע סייבר באופן עצמאי.

דוחות קשורים

- חדשנות טכנולוגית ואיומי סייבר מעצבים מחדש את סביבת הסיכונים של החברות, פברואר 2024
- נזקי המוניטין בעקבות מתקפות סייבר עלולות לגבות מחיר עסקי מחברות, אוקטובר 2020

הדוחות מפורסמים באתר מידרוג www.midroog.co.il

תאריך הדוח: 06.01.2026