

# אחריות הדירקטוריון

## בנושא הסייבר

### גילוי דעת



מאת: משה וולף, אל"מ במיל ולשעבר מנכ"ל שב"א ומס"ב. עו"ד עמית אשכנזי מרצה ויועץ בתחומי סייבר פרטיות ובינה מלאכותית, (לשעבר היועץ המשפטי של מערך הסייבר הלאומי ושל הרשות להגנת הפרטיות). אסף טורנר, מומחה הגנת סייבר והגנת הפרטיות, מנכ"ל מיה סקוורטי ויובל שגב, יו"ר פורום הסייבר באיגוד הדירקטורים (לשעבר ראש אגף טכנולוגיות מתקדמות במערך הסייבר הלאומי). ינואר 2023

#### דיסקליימר

האמור בנייר עמדה זה אינו חוות דעת משפטית או מקצועית וללא נועד להחליף ייעוץ משפטי או טכנולוגי בהתאם לנסיבות הארגון. האמור בנייר זה, הינו עמדתם המקצועית של הכותבים.

## תוכן עניינים

3..... קהל היעד ותכלית  
 3..... רקע  
 3..... התמודדות עם סיכוני סייבר  
 6..... הסייבר איננו איום תיאורטי  
 7..... אירועי סייבר כסיכון מהותי לארגונים  
 8..... התייחסות הרגולטורים לחובות הדירקטוריונים בנושא הסייבר  
 8..... חבות דירקטוריון בעולם, ובארץ  
 8..... השלכות המצב הקיים  
 9..... אחרית דבר - מסקנות והמלצות אופרטיביות  
 9..... אופרטיבי  
 10..... נספח א – נושאים בחרים לדוגמא, בהם ראוי כי יתקיים דיון בדירקטוריון  
 10..... נספח ב - מיפוי עיקרי החובות בנושאי סייבר החלות על חברי הדירקטוריון, בהתאם למאסדרים (רגולטורים) השונים בישראל  
 11..... נספח ג' – דוגמא לעקרונות מכוונים עבור בניית תכנית אכיפה פנימית בנושא

מובילות מקצועית  
 לדירקטורים מכהנים  
 על פי סקר ה-GNDI

## קהל היעד ותכלית

מסמך זה פונה בראש ובראשונה אל חברי דירקטוריון, במטרה להציע להם מתווה ישים להתמודדות עם החשיפה לסיכוני הסייבר הגוברים לפעילות החברות בהן הם מכהנים. המסמך מציג באופן כללי את מאפייני החשיפה, מורכבותה המשפטית והמקצועית, ואי הבהירות הרגולטורית ביחס למצופה מהדירקטור. על רקע האמור המסמך מציע לדירקטור תכנית פשוטה ליישום שמטרתה ביצוע תפקידו תוך צמצום החשיפה העסקית והמשפטית הנובעת מסיכוני הסייבר.

## רקע

הכללים החלים בדיני התאגידים בתחום הממשל התאגידי בכלל<sup>1</sup>, והחובות על דירקטורים בפרט, מצויים בתנופה בשנים האחרונות. אכן, כפי שמצטט פרופסור גרוס<sup>2</sup> את בית המשפט העליון באחת הפרשות ביחס לאחריות המקצועית של הדירקטור:

**"הדירקטור של שנות האלפיים אינו יכול להיות תם שאינו יודע לשאול שמדמן לפרקים להסב בצוותא ולשתות תה. הדירקטור בימינו נושא באחריות מקצועית על פי המבחן של נושא משרה סביר."**<sup>3</sup>

כידוע יסוד עקרוני בדיני התאגידים הוא הקשר שבין המשקיעים (בעלי המניות) המצפים לתשואה על השקעתם, לבין מי שמייצגים אותם בפעילות החברה, הדירקטוריון והנהלה. הדירקטוריון והנהלה את הנכסים שהופקדו בידם בתמורה לתגמול כספי, ומחויבים לפעול לטובת החברה.

על מנת להבטיח את הקשר האמור, קובע הדין חובות זהירות ומיומנות על הדירקטורים, וכן חובת אמון על מנת שלא ימעלו בתפקידם<sup>4</sup>. לצד כללים אלה, נקבע לדירקטורים מרחב שבו הדין אינו מתערב, הידוע כ- "כלל שיקול הדעת העסקי". כלל זה מבטא את התובנה שהדירקטורים מתמנים לתפקידם על מנת להשיא את הרווחים של המשקיעים בפעילות העסקית, וכי השאת רווחים בחיי המסחר המודרניים כרוכה לעתים כרוכה בלקיחת סיכונים. עקב כך, נזהרו בתי המשפט בעת ייחוס אחריות לדירקטורים לכישלונות עסקיים. זאת מתוך הבנה כי לבתי המשפט אין יתרון בקבלת החלטות עסקיות, וכי יש להיזהר מהטלת אחריות בדיעבד, אשר עלולה להביא לצמצום הנכונות לקחת סיכונים עסקיים ולסרבול הליך קבלת ההחלטות העסקי. גישה זו משקפת גם את מגוון הסיטואציות העסקיות האפשריות והחשיבות של בחינת הדברים בהתאם להקשר.

כאמור בפתיח, הכללים בתחום הממשל התאגידי מצויים בשינוי מגמה, בכך שבתי המשפט משרטטים את הקווים המנחים לגבי חובות הזהירות והאמון של הדירקטור והנגזר מכך להליכי קבלת ההחלטות בדירקטוריון ולאופן תיעודם.

## התמודדות עם סיכוני סייבר

אנו סבורים כי במציאות הטכנולוגית והעסקית הנוכחית, לדירקטורים חשיפה משפטית הנובעת מהצורך להתמודד עם סיכוני סייבר. כפי שנציג להלן, המוקד של חשיפה זו הינו הצורך בתשומת לב ניהולית, מודעת, מתועדת ומעודכנת לנעשה בתחום זה בתאגיד. המשמעות אינה מניעה מוחלטת של תקיפות סייבר, או הפיכת הדירקטורים למומחי סייבר. הדגש המרכזי הוא קיום ניהול סיכונים מסודר ומתועד, בעל זיקה עובדתית ומקצועית לפעילות התאגיד.

נציג להלן תחילה את החשיפה, ולאחר מכן את אופן ההתמודדות המוצע עמה

סיכוני הסייבר הם נגזרת של המרכזיות של טכנולוגיית המידע והתקשורת בפעילות העסקית המודרנית, ועם הדיגיטציה המואצת של ארגונים רבים כחלק מהתמודדות עם משבר הקורונה, כך עלתה החשיפה של הארגון. תקיפת סייבר מוצלחת כנגד חברה

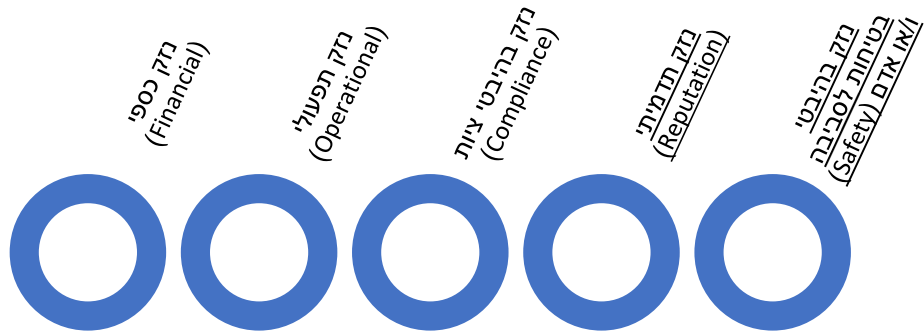
<sup>1</sup> ההתייחסות במסמך זה היא לחברות פרטיות שחל עליהן חוק החברות, התשנ"ט-1999 בלבד, וכן על תאגידים שחל עליהם חוק ניירות ערך, תשכ"ח-1968.

<sup>2</sup> יוסף גרוס, דירקטורים ונושאי משרה בעידן הממשל התאגידי, (מהדורה חמישית), נבו, 2018, (להלן – גרוס) בעמוד 241-2.

<sup>3</sup> רע"א 4024/14 אפריקה ישראל להשקעות בע"מ נגד כהן, פסקה 53, המצוטט בגרוס, 245.

<sup>4</sup> ראו, גרוס, עמוד 241.

עסקית כלשהי, ללא קשר לתחום עיסוקה, פריסתה והיקפה, עלולה להוביל לנזקים שונים לפעילות החברה, נכסיה, עובדיה, צדדים שלישיים, ואף למדינת ישראל, באחד או יותר מהמישורים הבאים:



כל אחד ממעגלי סיכון אלה, מצוי בדיקה לחובות החלות כבר כיום על הדירקטוריון בהכוונה של פעילות התאגיד ובפיקוח עליה. חובות אלה יכולות לנבוע מפרשנות חובת הזהירות<sup>5</sup> והמיומנות של הדירקטור בתאגיד מודרני הנשען על טכנולוגית מידע בכך שלא התמודד כראוי עם הסיכונים, או מהפרת חובת האמון במקרה שמדובר בחובות הנבעות מהפרה של החוק.<sup>6</sup> בהמשך למגמה בפסיקה בדיני התאגידים בדלוור, **ד"ר רועי שפירא סבור כי אי התמודדות של הדירקטוריון עם אירוע סייבר בעל השפעה על פעילות קריטית של התאגיד, עשויה להוביל לחשיפה לדירקטורים גם מבלי שהתאגיד כפוף לרגולציית סייבר כלשהי.**<sup>7</sup> לעמדתו של שפירא ייתכן שרף החבות להטלת אחריות יהיה גבוה, אולם במסגרת הבחינה המשפטית ייבדקו היבטים אלה: האם הדירקטוריון קיים דיון בסיכוני הסייבר, האם קיימו בקרה על ההנהלה בנושא זה, והאם התעלמו מ- "דגלים אדומים" שהובאו לידיעתם. עקב כך, גם מבלי שדיני התאגידים בהכרח דורשים התייחסות לסיכוני הסייבר, ניתן לומר כי בהתרחש אירוע סייבר בתאגיד שיגרם לאחד או יותר מהנזקים שתוארו, צפויות לעלות שאלות אודות אחריות הדירקטורים לכך, והחלק שלהם במניעה והתמודדות עם האירוע ותוצאותיו.

אנו סבורים כי זו תוצאה זו קשורה גם לתפקיד החשוב של טכנולוגיית מידע בחיי התאגיד. על מנת לקדם משק תחרותי ומתקדם, תאגידים נדרשים ליישם טכנולוגיות דיגיטליות. מיקסום התועלות מטכנולוגיות אלה טעון התמודדות עם הסיכונים הכרוכים בהם. בנוסף במשק תחרותי ומתקדם יש קשרי הגומלין בין פעילויות של ארגונים ובין ענפים, באופן שארגון אחד עלול להיות אמצעי לפגיעה בארגון אחר. במשק כזה אין מקום לאפשר "ויתור" על ניהול סיכוני סייבר בשם שיקול הדעת העסקי, משום שרמת הוודאות של הסיכון למשקיעים, לקוחות וצדדים שלישיים, היא גבוהה. ברמה המעשית, התמודדות עם סיכוני סייבר שונה מ-

<sup>5</sup> בהתאם לסעיף 252 לחוק החברות, חלה על הדירקטור חובת זהירות כלפי החברה, ובהתאם לסעיף 253 לחוק, מובהר כי הרף הינו גבוה יותר:

253. "נושא משרה יפעל ברמת מיומנות שבה היה פועל נושא משרה סביר, באותה עמדה ובאותן נסיבות, ובכלל זה ינקוט, בשים לב לנסיבות הענין, אמצעים סבירים לקבלת מידע הנוגע לכדאיות העסקית של פעולה המובאת לאישורו או של פעולה הנעשית על ידיו בתוקף תפקידו, ולקבלת כל מידע אחר שיש לו חשיבות לענין פעולות כאמור."  
ראו: גרוס, עמוד 244.

<sup>6</sup> ראו באופן כללי את הדיון המקיף והרלבנטי של ד"ר רועי שפירא:

משפט ועסקים כד 559. Director Oversight Duties (January 21, 2021) מחדל בפיקוח וחובת ההשגחה, Shapira, Roy (2021), Available at SSRN: <https://ssrn.com/abstract=3770579> or <http://dx.doi.org/10.2139/ssrn.3770579>

(להלן – שפירא, מחדל בפיקוח)

<sup>7</sup> Shapira, Roy, Mission Critical ESG and the Scope of Director Oversight Duties (May 12, 2022). 2022 Columbia Business Law Review (Forthcoming), Available at SSRN: <https://ssrn.com/abstract=4107748>

(להלן – Shapira, Mission Critical ESG), בעמוד 24.

"שיקול הדעת העסקי", במובן זה שבדומה לאופן ניהול הסיכונים החשבונאי, קיים ידע מקצועי נרחב על אופן ההתמודדות עם סיכוני הסייבר, ויש חשיבות רבה ליישומו בתאגיד.

על רקע האמור הנחת העבודה הינה כי על הדיקטוריון לנקוט אמצעים להתמודדות עם איומי סייבר, ואי נקיטה באמצעים אלה, עלולה להיות הפרה של חובת הזהירות והמיומנות, או אף הפרה של חובת אמון עקב מחדל בפיקוח. בהמשך לכך, בקרות אירוע סייבר, ניתן להעריך כי הדיקטוריון יידרש להראות מהן הפעולות שנקט, אם בכלל, כדי להיערך לסיכון הסייבר, ולכן לקיום הדיון האמור באופן מתועד ומסודר יש חשיבות רבה לצורך הגנה על הדיקטורים<sup>8</sup>. למסקנה זו ניתן להגיע גם מהחובה על הדיקטוריון לנהל סיכונים. כפי שכותב פרופסור גרוס, אין מקום להשאיר את ניהול הסיכונים בתחום הטכנולוגיה לשיקול הדעת של אנשי הטכנולוגיה בלבד.<sup>9</sup>

יודגש כי האמור כאן אינו מצביע על הצורך להעדיף תמיד את שיקולי הגנת הסייבר למול התועלת הארגונית משימוש בטכנולוגית מידע, כי אם לקיים על האמור דיון מסודר, מקצועי ומבוסס, המאפשר לדיקטוריון לקבוע מדיניות ניהול סיכונים ראויה.

ללא דיון כאמור בדיקטוריון, סיכון תפעולי משמעותי של הארגון אינו חשוף בפניו, לא זוכה לתשומת לב ולא בהכרח זוכה למשאבים והאמצעים הארגונים הנדרשים לצורך התמודדות עמו. לעומת זאת, דיון בדיקטוריון מאפשר לחברי הדיקטוריון לממש את אחריותם, וגם להפעיל את שיקול דעתם אודות מדיניות ניהול הסיכונים של התאגיד בתחום טכנולוגית המידע. דיון שכזה, מפחית את החשיפה לסיכון בעל מורכבות כמו סיכון הסייבר<sup>10</sup>.

על הדיקטוריון להתוות את המדיניות התאגידית בנושא, ולפקח על ביצועה, במסגרת חלוקת העבודה ושגרות העבודה עם יתר בעלי התפקידים בתאגיד<sup>1</sup>.

הדילמה העולה בתחום ניהול סיכוני הסייבר הינה שמדובר בתחום מקצועי הדורש מומחיות לצורך הבנת הסיכון, ולצורך איתור האמצעים והבקורות לצמצומו. עקב כך, יש נטייה בארגונים רבים לטפל בנושא זה במסגרת מקצועית שאינה מגיעה לדיוני דיקטוריון. בנוסף, דיקטורים רבים נרתעים מעיסוק בנושא זה, שאינו הסיבה שמונו לתפקידם. דיקטורים רבים מגיעים לתפקידם מכוח מומחיות ניסיון או הבנה בתחום הפעילות של התאגיד, ואלה אינם בהכרח כרוכים בהבנה של תחום טכנולוגית המידע או סיכוני הסייבר.

עיון ברגולציה הישראלית, מעלה כי נמצא בה פירוט חלקי לתוכן של אותן חובות. בתחום הבנקאות, דומה כי פירושה של החובה מוסדר באופן מעמיק בהוראות הניהול הבנקאי התקין השונות, החלות הן על פעילויות עסקיות וניהול סיכונים באופן כללי, הן על שימוש בטכנולוגית מידע, ולעיתים אף בהקשר ניהול סיכונים ספציפי כגון התהליך הנדרש למעבר לענן ציבורי, וחלוקת העבודה שבין הדיקטוריון והנהלה לבין יתר אגפי הארגון (וכך גם בטיטוט החוזר של רשות שוק ההון בנושא).

עם זאת, הוראות מפורטות מעין אלה אינן קיימות באופן כללי כחלק מדיני התאגידים. רשות ניירות ערך הצביעה לאחרונה על הצורך בקיום דיון בהנהלה בנושא, כאשר לסיכון הסייבר עלולה להיות השפעה על פעילות התאגיד, שהינה בעלת השלכה על שיקול הדעת של משקיע סביר.

<sup>8</sup> ראו שפירא- מחדל בפיקוח, בעמוד 17 המסכם את הכלל "לא תיעדת – לא השגחת".  
<sup>9</sup> גרוס, עמוד 212.

<sup>10</sup> ראו את דבריו של פרופסור גרוס, לגבי חובת הזהירות המוגברת, אשר מהווים השלד הכללי לדיון זה:  
" א. מידת המעורבות בתהליך שקדם להחלטה;  
ב. האם אסף את המידע הרלוונטי לצורך ההחלטה;  
ג. האם התעדכן במידע הקשור לפעילות החברה;  
ד. האם גילה בקיאות בענייניה;  
ה. האם התמצא במצבה הפיננסי;  
ו. האם נוכח בישיבות הדיקטוריון וכיוצא באלה נושאים." גרוס, עמוד 257.

מעין בדו"ח כספי של תאגיד שעבר תקיפת סייבר במהלך שנת 2022<sup>1</sup> עולה כי רשות ניירות ערך מתחה ביקורת על כך שהתאגיד לא קיים כלל דיון בדיקטוריון על אודות החשיפה שלו לסיכונים סייבר ואופן ההתמודדות עמם, ודיונים שנערכו בתאגיד לא בוצעו בהתאם לתפיסה שיטתית של ניהול סיכונים סייבר. בהתאם לאמור בדו"ח, החברה קיימה דיון רק לאחר שעברה תקיפת סייבר משמעותית, שבעקבותיה היא מבצעת מהלך מקיף באמצעות מומחים לאיתור סיכונים וצמצומם.

מקרה זה עלה לכתורות, וכך נכתב בכלכליסט<sup>11</sup>:

"דו"ח הדיקטוריון של החברה חושף כי ייתכן שניתן היה למנוע את השבתת פעילותה של הקבוצה המחזיקה בספנות ישראל בתחילת ינואר השנה עקב פריצת סייבר שביצעו האקרים פרו-פלסטינים. בנוסף, הוא קובע כי "החברה לא עמדה בחובת הדיווח המוטלת עליה" באשר לסיכון זה"

### קווים מנחים לצמצום החשיפה לסיכונים סייבר

אנו סבורים כי נדרש לייצר רף ציפיות המגדיר קווים מנחים של תהליך קבלת החלטות ומדיניות ארגונית בתחום הסייבר, המהוות רף מתאים להתמודדות נאותה עם איום הסייבר. בהיעדר רף מסוג זה ברמה הרגולטורית, מוטב יעשו דיקטוריונים אם יקיימו דיון ייעודי בנושא ויגדירו בצורה סדורה ומתועדת את הרף אותו הם מחילים על התאגיד. בלשונו של המלומד גרוס בהקשר לחובת הזהירות המוגברת של הדיקטור: "...יש להציב לנושא המשרה תמרום ברורים לאורם יפעל"<sup>12</sup>.

בהתאם לכך הקווים מנחים מוצעים כביררת מחדל מנחה את הדיקטורים. הם מאפשרים לדיקטוריון עם זאת, בהתבסס על בחינה ודיון מתאים, לקבוע את נקודת האיזון באופן אחר, אולם זאת תוך הצורך לנמק את הדברים. הם מייצרים ודאות ומונעים אפקט מצנן לשימוש בטכנולוגיה. מאליו מובן כי על פי התובנות המקובלות בתחום הגנת הסייבר, נקיטת אמצעים אלה בידי הדיקטוריון, ובהם איתור סיכונים סייבר המשמעותיים, גיבוש אמצעים הנדרשים לצמצום האמצעים, תקצוב מתאים, קביעת נהלים וביצוע בקרה, יש בהם כדי לצמצם את החשיפה של התאגיד לסיכונים סייבר. תובנה מקובלת בתחום הגנת הסייבר הינה כי נדרש לקבוע נהלים ובקורות על הגורם האנושי, המייצר חלק משמעותי מהסיכון. שילוב נהלים ובקורות אלה כחלק מהמארג התאגידי של ממשל תאגידי, כגון למשל תוכניות ציות פנימי<sup>13</sup>, מהוות מכפיל כוח.

בהתאם לסעיף 266 לחוק החברות דירקטור זכאי לקבל סיוע מקצועי בעת ביצוע תפקידיו, ויש להזכיר הוראה זו גם ביחס לחובות הדיקטור המתוארות לעיל<sup>14</sup>. גם בנושא זה, יש תועלת בהפניה למאפיינים המרכזיים של אותו מומחה, על מנת לסייע לדיקטור במילוי חובותיו. זאת על רקע העובדה שתחום הגנת הסייבר הינו תחום חדש יותר ולא תמיד ברור איזו מומחיות נדרשת, וזאת בשונה מיועץ שהינו עורך דין או רוהה חשבון.

דוגמאות לשאלות מרכזיות למצוא [בנספח א'](#).

## הסייבר איננו איום תיאורטי

כאשר מדובר בתאגידים על פי הערכות מומחים, עלויות פשעי הסייבר העולמיות יגדלו ב-15% בכל שנה בחמש השנים הבאות. עלויות אלה יגיעו ל-10.5 טריליון דולר בשנה עד 2025, לעומת 3 טריליון דולר ב-2015<sup>15</sup>. מציאות זו, מתאפיינת בקצב גידול אקספוננציאלי, משמעותית יותר מהנזק הנגרם כתוצאה מאסונות טבע בכל שנה, ופשעי סייבר יהיו רווחיים יותר מהסחר העולמי בסמים הבלתי חוקיים.

<sup>11</sup> <https://www.calcalist.co.il/calcalistech/article/sk11lvswj>

<sup>12</sup> גרוס עמוד 257.

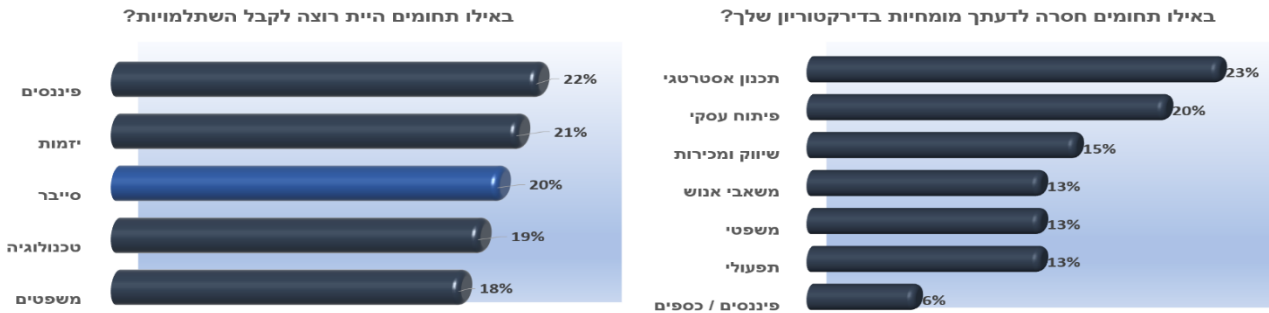
<sup>13</sup> ראו למשל: פרקליטות המדינה, מדיניות התביעה בהעמדה לדיון וענישה של התאגיד, הנחיות פרקליט המדינה 1.14 (תש"פ), עמוד 17.

<sup>14</sup> ראו גם גרוס, בעמוד 265.

<sup>15</sup> <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021>

על פי סקר אותו יזם איגוד הדירקטורים במהלך שנת 2022<sup>16</sup>, עלה כי אחד מתוך ששת הדברים אותם מגדירים חברי דירקטוריון כחשובים ביותר לשיפור בדירקטוריון, הינו הרחבת רמת האחריות שלהם.

**עוד עלה בסקר, כי הם אינם מזהים את הסייבר כמומחיות חסרה, אלא בנושא בו היו רוצים לעבור השתלמויות.**



כיום, הדרך של דירקטוריונים להתמודד בצורה נאותה עם אתגרי הסייבר נתונה לפרשנות מרחיבה. אמות המידה לבחינה האם הדירקטוריון פעל בצורה נאותה עשויות להיות מוטות מהסערה התקשורתית, מאינטרסים של בעלי עניין ומגורמים שונים ומגוונים. חברי דירקטוריון רבים מבינים כי תחום הסייבר מונח על שולחנם, אך שיטת הפעולה ודרך הפיקוח והבקרה הנדרשים מהם בנושא, לעיתים לוטים בערפל. מציאות זו, מייצרת שונות גדולה מאוד באופן בו נוקטים דירקטוריונים לניהול הסיכון ומקשה על נושאי המשרה להבין כיצד עליהם לפעול.

## אירועי סייבר כסיכון מהותי לארגונים

בסקרים שונים עולה כי המודעות לחשיבות ההגנה בסייבר בתאגיד הינה גבוהה. חברי דירקטוריונים רבים מעידים כי הסייבר הינו סיכון מהותי, שנבחן על ידם ומקבל מענה. כך לדוגמה בסקר משנת 2021 של גרטנר<sup>17</sup>, עלה כי 88% מהמשיבים, אמרו כי הם רואים בסייבר סיכון עסקי, וכ-66% מחברי הדירקטוריון שהשתתפו בסקר של הבורסה לניירות ערך בניו-יורק<sup>18</sup> הגדירו כי הם לא מרגישים בטוחים לגבי רמת ההגנה בסייבר של התאגיד.

בהיבט זה, יש לציין את ניסיון סחיטה מצד עובד לשעבר של חברת לאומי קארד באוקטובר 2014, בדרישה לתשלום בסך של 3 מיליון שקלים בתמורה לאי פרסום מאגר הנתונים של 1.5 מיליון לקוחות החברה. לפי פרסום בעיתונות הכלכלית, בעיצומו של האירוע, יו"ר בנק לאומי, ברודט, שלח (5 בנובמבר 2014) מכתב לפרקליט המדינה, בהמשך לפגישה שקיים עמו יום קודם לכן בנושא, וציין בו כי (ההדגשות של כותבי המסמך): "עלול להיגרם זנק עצום לציבור לקוחות הבנק **מעצם פרסום האפשרות שמידע בנקאי על לקוחות הבנק יפורסם ברחבי האינטרנט**, אף אם מאגר המידע לא יופץ בסופו של דבר. ההיסטוריה הציבורית שהפרסום עלול לעורר תביא, ברמת הסתברות גבוהה, **לאובדן אמון ולכאוס במערכת הבנקאית, ללא קשר להתממשות האיומים**". מנכ"לית הבנק באותה עת, רקפת רוסק-עמינח, צוטטה התייחסה במרץ אשתקד לאירוע זה וציינה: "אלה היו 16 הימים הכי קשים שהיו לי בקריירה. בפער".

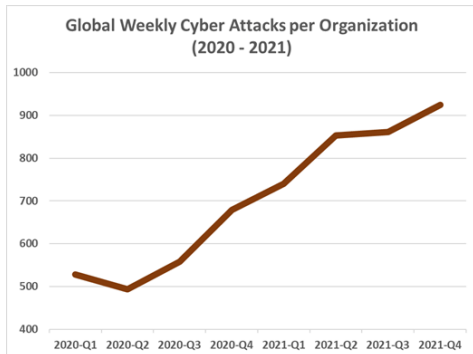
16

[https://www.idu.org.il/images/%D7%A1%D7%A7%D7%A8\\_%D7%93%D7%99%D7%A8%D7%A7%D7%98%D7%95%D7%A8%D7%99%D7%AA\\_2022\\_%D7%93%D7%95%D7%97\\_%D7%9E%D7%9C%D7%90\\_3.pdf](https://www.idu.org.il/images/%D7%A1%D7%A7%D7%A8_%D7%93%D7%99%D7%A8%D7%A7%D7%98%D7%95%D7%A8%D7%99%D7%AA_2022_%D7%93%D7%95%D7%97_%D7%9E%D7%9C%D7%90_3.pdf)

<https://www.gartner.com/en/newsroom/press-releases/2021-11-18-gartner-survey-finds-88-percent-of-boards-of-directors-view-cybersecurity-as-a-business-risk>

[https://www.nyse.com/publicdocs/VERACODE\\_Survey\\_Report.pdf](https://www.nyse.com/publicdocs/VERACODE_Survey_Report.pdf)

מערכות המידע מניעות ומאפשרות את כל היבטי התפעול בארגון, פגיעה בהן על ידי התקפת סייבר עלולה לגרום לאובדן הכנסות, הפסקה בייצור, עלייה בפרמיות ביטוח, קושי בקבלת אשראי, ירידת ערך מניה ועוד. סיכוני סייבר מאיימים לא רק על מערכות המידע בארגון אלא גם על התהליכים העסקיים שלו ועל עתידו ממש. בארץ ובעולם מספר התקפות הסייבר עולה באופן קבוע ואיתו גם החברות והארגונים שקרסו כתוצאה מהתקפת סייבר. עם זאת ניהול סיכוני סייבר בארגון נשאר לרוב בידיו של מנהל ה-IT או מנהל אבטחת מידע בהנחיית המנכ"ל כאשר מקבלי החלטות האמונים על ניהול כלל הסיכונים בארגון נשארים פעמים רבות "מחוץ לתמונה".



ה-IT או מנהל אבטחת מידע בהנחיית המנכ"ל כאשר מקבלי החלטות האמונים על ניהול כלל הסיכונים בארגון נשארים פעמים רבות "מחוץ לתמונה".

כאשר רמת המורכבות של ניהול סיכוני סייבר עולה ואיתה גם הפגיעה האפשרית מהתקפה קשה, קבלת החלטות צריכה להתבצע על ידי אותם אנשים הרגילים בניהול סיכונים ומודעים למתרחש בארגון על כל היבטיו – הדיקטוריון. מחקר של חברת צ'קפוינט משנת 2021<sup>19</sup>, מציג כי כמות התקיפות הממוצעות שחווים ארגונים עולה בהתמדה.

## התייחסות הרגולטורים לחובות הדיקטוריונים בנושא הסייבר

### חבות דירקטוריון בעולם, ובארץ

באירופה ובארה"ב פסקי דין עוסקים בדיקטוריון עצמו וניתן להזכיר את עניין Caremark בו הוטלה על חברי הדיקטוריון אחריות אישית על מחדל בפיקוח, התביעות הייצוגיות בענייני MyHeritage, Facebook<sup>20</sup>, Yahoo<sup>20</sup> קנסות שונים כדוגמת British Airways<sup>22</sup> ועוד אשר שמו את חברי הדיקטוריון כאחראים האולטימטיביים להגנת הפרטיות ולביטחון מערכות המידע של ארגוניהם.<sup>23</sup>

בארץ, ישנן שתי רגולציות דומיננטיות "חוצות מגזר". תקנות אבטחת המידע של הרשות להגנת הפרטיות וגילוי הדעת בדבר חובות גילוי ודיווח של הרשות לניירות ערך. שני הרגולטורים אמנם דורשים דיונים בהיבטי הגנת סייבר ודיווחים בזמן אמת על אירועי סייבר משמעותיים אך עם זאת אינם דורשים במפורש מעורבות אפקטיבית של הדיקטוריון עצמו. זאת למרות שהדיקטוריון חשוף לשלל תביעות וסנקציות בעקבות התקפות סייבר וביניהן תביעות של החברה נגד דירקטורים בעילה של הפרת חובת זהירות \ אמונים, תביעה נגד דירקטורים בנושאי פגיעה בפרטיות ועוד. בנוסף, המפקח על הבנקים הגדיר כחלק מהוראת ניהול בנקאי תקין 301 וכן 361 בנושא ניהול הגנת הסייבר מספר דרישות מוגדרות מחברי הדיקטוריון.

לעיון במיפוי הדרישות הרגולטוריות החלות על תאגידים שונים בישראל, ראה [נספח ב](#).

### השלכות המצב הקיים

על אף חשיבות הנושא והחשיפה המשפטית המצב בחברות רבות במשק הישראלי הוא של חוסר מעורבות של הדיקטוריון בכל הקשור למדיניות ומצב הגנת הסייבר בארגונם – אם מתוך חוסר כלים מקצועיים להתמודד עם הנושא ואם מתוך החלטה כי הנושא אינו מצריך את מעורבותם האישית. בתחילת השנה, פרסמה הרשות לניירות ערך בארה"ב (SEC) טיוטת כללים<sup>24</sup> שמטרתם להבהיר ולקבוע הוראות נוספות להיבטי הסייבר מנקודת המבט של הדיקטוריון. בין הנושאים המוצעים, התייחסה

<sup>19</sup> [/https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year](https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year)

<sup>20</sup> <https://www.natlawreview.com/article/court-approves-class-action-settlement-re-yahoo-inc-customer-data-security-breach>

<sup>21</sup> [/https://www.courthousenews.com/judge-advances-settlement-over-2018-facebook-data-breach](https://www.courthousenews.com/judge-advances-settlement-over-2018-facebook-data-breach)

<sup>22</sup> [https://www.fastcompany.com/90373254/british-airways-just-got-hit-with-a-massive-229-million-gdpr-fine?partner=rss&utm\\_source=twitter.com&utm\\_medium=social&utm\\_campaign=rss+fastcompany&utm\\_content=rss](https://www.fastcompany.com/90373254/british-airways-just-got-hit-with-a-massive-229-million-gdpr-fine?partner=rss&utm_source=twitter.com&utm_medium=social&utm_campaign=rss+fastcompany&utm_content=rss)

<sup>23</sup> ראו עוד Shapira, Mission Critical ESG.

<sup>24</sup> <https://www.sec.gov/rules/proposed/2022/33-11038.pdf>



הרשות בין היתר לנושאים כגון: מסירת מידע על הפיקוח שמבצע דירקטוריון התאגיד בנושא ניהול סיכונים סייבר, התפקיד שנוטלת הנהלת התאגיד בנושא זה והמומחיות הקיימת בנושא זה בהנהלה, גילוי בדבר מומחיות בתחום הגנת סייבר שיש למי מחברי דירקטוריון התאגיד ומהותה של המומחיות (אם קיימת), לרבות ניסיון עבר בתחום, הסמכה מקצועית רלוונטית או רקע אחר הקשור לתחום ועוד. הכללים מבהירים כי זיהוי מומחיותו של חבר דירקטוריון בתחום זה לא תטיל עליו כל אחריות מוגברת או שונה בתפקידו כדירקטור, ולא תפחית מהאחריות הרגילה שיש ליתר חברי הדירקטוריון.

כמובן שאין דין חברה בורסאית, כדן חברה פרטית, וכל דרישה צריכה להיות מידתית ותואמת את הסיכון.

רצוי היה לקיים דיון מסודר הבוחן את מכלול השיקולים, בידי גורם מדינתי מוסמך, ובאופן שיסייע לצמצם את אי הבהירות ויתמוך בהשקעה יעילה של משאבים בתחום זה. בהיעדר אמירה מסוג זה, על דירקטוריונים להגדיר לעצמם בצורה עצמאית מדיניות סדורה כתובה ומאושרת לנושא. מדיניות זו, תשקלל את הצעדים הנדרשים לביצוע במסגרת עבודת הדירקטוריון הן בראיה העסקית והן ברמת ההשלכות החיצוניות לבעלי העניין של התאגיד.

מדיניות כזו, עשויה לכלול התייחסות לידע נדרש בקרב הדירקטוריון, תחומים אשר נדרשים לבוא לאישורם ועוד. תכנית זו, יכולה לכלול לדוגמה את הפרמטרים המובאים [בנספח ג'](#) למסמך זה.

## אחרית דבר - מסקנות והמלצות אופרטיביות

אין ספק כי האחריות על נושא הגנת הסייבר והפרטיות מונחת לפתחו של הדירקטוריון. יחד עם זאת, לאור אי הבהירות ומורכבות הנושא, ראוי כי דירקטוריונים יקיימו לכל הפחות דיון ייעודי שמטרתו קביעת מסגרת לעיסוק בנושא בתאגיד. מסגרת זו יכולה לכלול מספר צעדים פשוטים וברורים, דוגמת השתלמות, אישור תקציב ותוכניות עבודה, השתתפות בתרגולים עיתיים וצעדים נוספים כגון אלו המוצעים במסמך זה. בנוסף על הדירקטוריון פיקוח על כך שנקטו אמצעים סבירים ליישום המסגרת, וכי אין ממצאים מטרידים על קיום חשיפה לסיכונים סייבר. האיגוד עומד לרשות הדירקטוריונים בישראל, במטרה לסייע להם לממש את אחריותם, באמצעות מתן כלים, שיתוף בניסיון והעמדת ידע מקצועי.

## אופרטיבי

מלבד היות הדירקטוריון אחראי לניהול הסיכונים בארגון ומשכך – גם סיכונים סייבר, הדירקטוריון מהווה כוח קריטי לקידום הגנת סייבר בארגון ויצירת סביבה התומכת בתהליכים אלה. הדירקטוריון אחראי להכרה ולפיקוח על התהליכים הבאים:

1. הכנסת מומחיות סייבר לדירקטוריון על ידי צירוף חבר דירקטוריון בעל מומחיות סייבר או יועץ סייבר קבוע לדירקטוריון.
2. לקיחת אחריות פורמלית על התחומים הרלוונטיים בהגנת סייבר.
3. הערכת רמת הסיכון הקיימת לארגון על ידי ביצוע סקר סיכונים סייבר מטעם המבקר הפנימי/צד ג' בלתי תלוי. הערכה זו תכלול בין היתר את ניתוח נקודות התורפה של הארגון, זיהוי איומים ופגיעויות פוטנציאליות ויכולת תגובה לאירועים.
4. פיתוח תוכנית לניהול סיכונים סייבר המכילה את הפעולות שהארגון יבצע על מנת לצמצם ולנהל את סיכונים הסייבר. התוכנית תכלול בין היתר הטמעת בקורות ונהלי אבטחה מתאימים, מודעות עובדים והשקעה בטכנולוגיית הגנת סייבר ובתהליכים ארגוניים מתאימים.
5. הקצאת משאבים לניהול סיכונים סייבר בארגון. סיכונים אלו יכללו גם כאלו שמקורם בשרשרת האספקה/צד ג'.
6. סקירה עיתית של תוכנית הסייבר ועדכונה על פי הצורך על מנת להבטיח יעילות ורלוונטיות בטיפול באיומי סייבר קיימים ועתידיים. הסקירה תכלול בין היתר גם את הטכנולוגיות והתהליכים המשמשים בניהול סיכונים סייבר.
7. עריכת תוכניות הכשרה ומודעות קבועות על מנת ללמד את העובדים כיצד להתמודד עם איומי סייבר ולעודד התנהגות מקוונת בטוחה.
8. פיתוח ותרגול תוכנית תגובה במקרה של אירוע סייבר ברמה התפעולית וברמת הנהלה. התוכנית תכלול בין היתר את הצעדים לזיהוי, הכלה וטיפול באיום, וכן מזעור נזקים והתאוששות.
9. סקירה ועדכון על פי הצורך של כיסוי ביטוח הסייבר של הארגון על מנת להבטיח שהוא מספק הגנה מתאימה מפני איומי הסייבר הרלוונטיים לחברה.
10. מעקב ועדכון פרופיל סיכונים סייבר של הארגון במקביל לעדכונים שוטפים לגבי איומים ופגיעויות חדשים בעולם הסייבר, בסביבה העסקית ובסביבה הגיאוגרפית.

## נספח א – נושאים נבחרים לדוגמא, בהם ראוי כי יתקיים דיון בדירקטוריון

מן הראוי כי הדירקטוריון יהיה ער לשאלות הבאות:

- א. מהם הנכסים והפעילויות הקריטיים של הארגון התלויים בתפקוד תקין של מערכות המידע?
- ב. מהי רמת החשיפה של מערכות מידע אלה לסיכוני סייבר?
- ג. מהם האמצעים שננקטו לצמצום החשיפה ואילו פעולות ננקטו להתמודדות עם החשיפה (ובין היתר):
  - (א) מי בארגון מופקד על פעילות זו ומהם המשאבים העומדים לרשותו?
  - (ב) באיזו מידה זהו פונקציות ושירותים חיוניים והוטמעו תוכניות כדי להקנות להם את הגמישות במקרה שיתרחש שיבוש או אירוע סייבר לשוב למצבם התקין (resilience)?
  - (ג) האם מוקצה לנושא זה המשאבים המתאימים בהיבטי תקציב וכוח אדם?
  - (ד) כיצד מממשת ההנהלה את המדיניות בהיבטי נהלים, טכנולוגיה, וכוח אדם?
  - (ה) האם בוצעו ביקורות בלתי תלויות?
- ד. האם הדירקטוריון מקבל דיווחים ישירים מגורמי המקצוע הבכירים העוסקים בנושא כגון מנהל הגנת הסייבר?
- ה. האם הדירקטוריון נדרש לסיוע חיצוני לצורך פיקוח על עמידה באמור?
- ו. באיזו מידה קיימת הלימה בין מדיניות הגנת הסייבר לבין שינויים טכנולוגיים בעבודת הארגון והפעילות העסקית?
- ז. האם קרו אירועים חריגים המעידים על חשיפה או סיכון מוגברים?

## נספח ב - מיפוי עיקרי החובות בנושאי סייבר החלות על חברי הדירקטוריון, בהתאם למאסדרים (רגולטורים) השונים בישראל

| מאסדר             | מקור   | חובות עיקריות   |
|-------------------|--|---|
| הרשות לניירות ערך | <a href="#">עמדה משפטית מספר 33-105: גילוי בנושא סייבר</a>               | <ul style="list-style-type: none"> <li>* גילוי בתשקיף ובדו"ח תקופתי</li> <li>* דיון בגורמי סיכון:</li> <li>- יובא סיכום קצר של האיזונים, החולשות וגורמי הסיכון האחרים של התאגיד, הנובעים מסביבתו הכללית, מן הענף ומן המאפיינים הייחודיים שבפעילותו; הדיון יהא תמציתי ובהיר; בהצגת סיכונים כלליים אשר מטיבם חלים על כל תאגיד יש להסביר באופן ברור את השפעתם המיוחדת על התאגיד</li> <li>- יוצגו גורמי הסיכון, בטבלה, על פי טיבם - סיכוני מקרו, סיכונים ענפיים, סיכונים מיוחדים לחברה - וידורגו בקטגוריות על פי השפעתם, ככל שניתן לגבי כל גורם סיכון, לדעת ההנהלה, על עסקי התאגיד - השפעה גדולה, בינונית וקטנה".</li> <li>* גילוי על אירועים חמורים מעסקי התאגידים הרגילים</li> <li>* גילוי בדו"ח הדירקטוריון</li> <li>* גילוי בדיווחים מיידיים</li> </ul> |
| הרשות לניירות ערך | <a href="#">גילוי דעת 3/17: שיתוף מידע לצורך התמודדות עם איומי סייבר</a> | שיתוף מידע בין גופים מסחריים לצורך התמודדות עם איומי סייבר. לאור התגברות איומי הסייבר בשנים האחרונות, הולך וגובר הצורך של גופים וארגונים בשיתוף מידע שעשוי להועיל להם בהתמודדות עם איומים אלו, בייחוד בין גופים הפועלים בענף מסוים. שיתוף מידע בין מתחרים עשוי להוות, בנסיבות מסוימות, הסדר כובל על פי חוק ההגבלים העסקיים.   |
| המפקח על הבנקים   | <a href="#">ניהול בנקאי תקין 361</a>                                     | התאגיד הבנקאי יהיה אחראי על הנושאים הבאים: <ol style="list-style-type: none"> <li>(א) התווית אסטרטגית הגנת סייבר כלל תאגידית ואישורה</li> <li>(ב) אישור מסגרת לניהול סיכוני סייבר ומדיניות הגנת הסייבר התאגידית</li> <li>(ג) קביעת אופן המעקב והפיקוח על ההנהלה הבכירה, ביישום מסגרת ניהול סיכוני סייבר</li> <li>(ד) קבלת דיווח על אירועי סייבר משמעותיים</li> </ol>  |
| המפקח על הבנקים   | <a href="#">ניהול בנקאי תקין 301</a>                                     | לפחות דירקטור אחד יהיה בעל ידע וניסיון מוכח בתחומי טכנולוגית המידע הדירקטוריון ימנה "ועדה לענייני טכנולוגיית מידע וחדשנות טכנולוגית", ולפחות אחד מחברי הועדה יהיה בעל ידע וניסיון מוכח בתחום טכנולוגיית המידע. הועדה תקיים קשר עם מנהל טכנולוגיית המידע ומנהל אבטחת המידע כהגדרתם בהוראת ניהול בנקאי תקין מס' 357, עם מנהל הגנת הסייבר כהגדרתו בהוראת ניהול בנקאי תקין מס' 361, ועם הגורם האחראי על תחום החדשנות.   |

| מאסדר                      | מקור  | חובות עיקריות   |
|----------------------------|---|---|
|                            |   | <p>המפקח על הבנקים. הועדה תדון ותמליץ לדירקטוריון בנוגע לאישור הנושאים הבאים: (1) אסטרטגיה ומדיניות טכנולוגיית המידע וניהולה, לרבות אבטחת מידע וסייבר, התשתיות הטכנולוגיות של התאגיד הבנקאי, ניהול ושימוש במאגרי נתונים, חדשנות טכנולוגית לתמיכה בחדשנות עסקית, והתאמתן לאסטרטגיה ולמדיניות הכוללת של התאגיד הבנקאי (2) אופן היערכות התאגיד הבנקאי לבנקאות העתיד ולהתמודדות עסקית עם אתגרי חדשנות טכנולוגית בכלל וחדשנות משבשט בפרט. (3) מסגרת לניהול סיכונים טכנולוגיים, לרבות סיכוני אבטחת מידע וסייבר וסיכוני חדשנות (4) תוכנית התאוששות מאסון ומידת התאמתה לעקרונות מסגרת העבודה לניהול ההמשכיות העסקית (5) יעדים ותוכנית עבודה שנתית (6) הקצאת משאבים נאותה למימוש הפעילות המתוכננת של התאגיד הבנקאי בתחום טכנולוגיית המידע, ניהול המידע והחדשנות.</p>   |
| רשות שוק ההון ביטוח וחסכון | <p><a href="#">סיטת חוזר ניהול סיכוני סייבר בנותני שירותים פיננסיים</a></p> | <p>תפקידי הדירקטוריון</p> <p>1 מדיניות ניהול סיכוני סייבר דירקטוריון של נותן שירותים פיננסיים יקבע מדיניות לניהול סיכוני סייבר ובכלל זה: א. ידון ויאשר מדיניות כתובה לניהול סיכוני סייב. ב. ידון בתכנית מעודכנת לניהול סיכוני סייבר כמפורט בסעיף 3, לרבות השינויים שבוצעו בה, לכל הפחות אחת לשנה; ג. יאשר את כתב מינוי ועדת ההיגוי בתחום סיכוני סייבר שבמסגרתו יוגדרו תפקידיה וסמכויותיה של הוועדה</p> <p>2 פיקוח ובקרה דירקטוריון של נותן שירותים פיננסיים יפקח על אופן ניהול סיכוני הסייבר, בין היתר באמצעות כל אלה: א. יקבע סוגי דיווחים אשר נדרשים לדירקטוריון, בנוסף לדיווחים הנדרשים בהתאם לחוזר, בקשר לניהול סיכוני סייבר, לרבות בקורות אירועי סייבר, וכן יקבע את מועדי הדיווחים ומתכונת העברתם; ב. ידון בדוחות שהוגשו לו על ידי מנהל הגנת הסייבר, לפי סעיף 32ד3 סמוך למועד הגשתם, ויוודא שסיכוני הסייבר אשר הוצגו בדוחות מטופלים באופן ראוי; ג. יגדיר אירועי סייבר מהותיים, עליהם יש לדווח באופן מיידי לדירקטוריון ולמפקח על שירותים פיננסיים</p> |
| מערך הסייבר הלאומי         | <p><a href="#">תורת ההגנה בסייבר לארגון (גרסה 2)</a></p>                    | <p>אחריות הדירקטוריון לאישור הממשל התאגידי, אישור של מפת הסיכונים הארגונית והקצאת משאבים נאותים (כוח אדם ותקציב)</p> <p><b>הערה:</b> מסמך תורת ההגנה איננו מסמך מחייב עבור רוב המשק. יחד עם זאת, הוא מהווה בסיס למספר רגולציות בישראל, ורגולציות קיימות (דוגמת זו של הרשות לני"ע, משרד הבריאות ושל המשרד להגנת הסביבה מפנים אליו)</p>   |
| מערך הסייבר הלאומי         | <p><a href="#">ניהול סיכוני סייבר בסביבת OT מדריך לדירקטוריון</a></p>       | <p>אופן ניהול סיכוני הסייבר בסביבת הרשת התפעולית Operational Technologies - OT</p> <p>הרחבה זו נועדה לספק תשתית לדיאלוג מתמשך בין הדירקטוריון להנהלה בנושא</p>  |

## נספח ג' – דוגמא לעקרונות מכוונים עבור בניית תכנית אכיפה פנימית בנושא

| רמת סיכון גבוהה  | רמת סיכון בינונית  | מומחיות מקצועית של הדירקטוריון בתחום        |
|--|--|---|
| <p>מינוי חבר דירקטוריון בעל הבנה וניסיון בתחום טכנולוגי של לכל הפחות 8 שנים בתפקיד ניהולי כגון: CISO/CIO/CTO</p>   | <p>★ הסתייעות במומחה תוכן מקצועי חיצוני או מינוי חבר דירקטוריון בעל הבנה בטכנולוגיה / סייבר</p> <p>- עסק בתחום לכל הפחות חמש שנים</p> <p>- עבר השתלמות מקצועית בהיקף של 100 שעות לכל הפחות</p>   | <p>מומחיות מקצועית של הדירקטוריון בתחום</p> |
| <p>★ השתתפות בתרגול אירוע סייבר לכל הפחות אחת לשנה</p> <p>★ אישור הקצאת המשאבים (תקציב וכח אדם).</p> <p>★ הדירקטוריון יוודא פיקוח ובקרה אחר מימוש הקצאת המשאבים וכי לא פחותים מהמקובל בענף.</p> <p>★ אישור אייחוס התאגיד, רמת הסיכון המקובלת (תיאבון הסיכון) ומפת האיומים השנתית</p> <p>★ אישור אסטרטגיית הסייבר בתאגיד</p> <p>★ קבלת סקירה מקצועית רבעונית מהגורמים האמונים על הסייבר והפרטיות בארגון. סקירה זו תכלול לכל הפחות את סטטוס יישום ועמידה בחובות החלות על הארגון בתחום הסייבר והגנת הפרטיות</p> | <p>★ השתתפות בתרגול אירוע סייבר לכל הפחות אחת לשלוש שנים</p> <p>★ אישור הקצאת המשאבים (תקציב וכח אדם)</p> <p>★ אישור מפת הסיכונים הארגונית</p> <p>★ קבלת סקירה מקצועית שנתית סטטוס יישום ועמידה בחובות החלות על הארגון בתחום הסייבר והפרטיות</p> | <p>חובות עיתיות</p>                         |