רשות ניירות ערך
Israel Securities Authority
سلطة الأوراق المالية

עמדת סגל

י״ב חשון תשע״ט
21 אוקטובר 2018

עמדות סגל הרשות המובאות להלן הינן עמדות מקצועיות המשקפות החלטות ועמדות של הסגל בסוגיות הנוגעות ליישום דיני ניירות ערך. תוכן העמדות המפורסמות מנחה את הרשות והסגל בהפעלת סמכותם והציבור יוכל להשתמש בהן ולהחילן בנסיבות דומות.

עמדה משפטית מספר 33-105: גילוי בנושא סייבר

ביום 25 בינואר 2023 עודכנה עמדת הסגל. השינויים העיקריים שבוצעו (מסומנים באפור) – הוספת תמצית ממצאי ביקורת סייבר שנערכה בתאגידים מדווחים, עדכון הגדרת "תקיפת סייבר", הוספת פרק גילוי על מדיניות ניהול סיכוני סייבר, הוספת פרק גילוי על מומחיות נושאי משרה וחברי דירקטוריון בפיקוח וניהול סיכוני סייבר, הבהרת אופן בחינת מהותיות דיווח מיידי אודות אירוע סייבר

א. מבוא

בשנים האחרונות עלה נושא ההתמודדות מול איומי הסייבר לסדר היום הציבורי והתאגידי. הדבר נובע, בין היתר, מאופיין של תקיפות הסייבר שהפכו עם השנים למתוחכמות והרסניות יותר ויותר. קצב השינויים המהיר בעולם הטכנולוגי כמו גם החדשנות וזמינות המידע, יוצרים הזדמנויות עסקיות מגוונות, וכן יוצרים לעיתים תלות בכלים מחשוביים אשר לא אחת מסופקים או מתוחזקים על ידי גורמים חוץ ארגוניים. עולם זה מייצר חשיפות ואיומים חדשים שלעיתים קשים לזיהוי ודורשים מומחיות באיתורם, במניעתם, בהתאוששות מפגיעתם ובמזעור נזקים.

חשיפה לאיומי סייבר עשויה לנבוע מסוגים שונים של תקיפות ומגורמים שונים של מתקיפים, פנים ארגוניים וחוץ ארגוניים, הפועלים כלפי התאגיד עצמו או גורמים הקשורים אליו. תקיפות הסייבר לובשות צורות שונות כאשר כיום הנפוצות ביותר הן: DOS (מניעת שירות), שיטוי עובדים ותקיפות אחרות תוך שימוש בדואר אלקטרוני או תוכנות זדוניות. תוצאת התקיפות היא בין היתר, גניבה, פגיעה (מחיקה, הצפנה) או שיבוש של מידע, השחתת אתרי אינטרנט, גניבת כסף (במסחר בבורסה, בנקים, חברות ביטוח) ועוד.

היקף החשיפות לאיומי סייבר משתנה מתאגיד לתאגיד ותלוי בגורמים רבים ומגוונים. בין הגורמים ניתן לציין - מצב פוליטי-מדיני, תחומי פעילות, גודל, רגישות המידע הקיים בתאגיד, תלות התאגיד בכלים מיחשוביים, אופן שמירת הנתונים וזרימת המידע בתאגיד, וגורמים נוספים שיש בהם כדי להגביר את המוטיבציה לפגיעה בתאגיד.

תקיפת סייבר יכולה להתבטא בנזקים ישירים ועקיפים ובהם – אובדן הכנסות, פגיעה ברכוש מוחשי (כגון גניבת כסף, אובדן מלאי) וברכוש בלתי מוחשי (כגון במקרה של גניבת פטנטים או זכויות יוצרים), פיצוי ללקוחות נפגעים, עלויות משפטיות בשל תביעות צדדי ג' שניזוקו וכדומה. פגיעה במוניטין, הוצאות השיקום ובהם שחזור מידע, הגדלת פרמיות ביטוח ועלויות להגברת הגנות סייבר במקרה של נזקי סייבר, עלולות אף הן להיות מהותיות. כמו-כן, קיים סיכון בתקיפת סייבר למהימנות המערכות החשבונאיות בארגון, באופן שעלול לפגוע בדיווח הכספי או ביכולת הבקרה עליו.

במקרים מסוימים עלולים הנזקים הכלכליים והעסקיים כתוצאה מתקיפות הסייבר להגיע להיקף משמעותי ביותר ועד כדי פגיעה ביכולת של התאגיד לעמוד בהישגים וביעדי שירות (רציפות תפקודית) ובהמשכיות העסקית שלו. בנוסף, התאוששות וריפוי הנזקים יכול שיִמשכו זמן רב עד חזרת התאגיד לפעילות תקינה, אם בכלל.

זאת ועוד, השפעת איומי הסייבר כסיכון משתנה תדיר, עלולה להיות מהותית לתאגיד אף אם לא התממשו האיומים וזאת למשל כתוצאה מעלויות הכרוכות בשיפור או בחיזוק מערך הגנת הסייבר. ייתכנו גם עלויות עקיפות נוספות כגון כתוצאה מהאטת תהליכים בתאגיד שתנבע משינוי נהלי האבטחה הפנים ארגוניים.

בישראל קיימים מספר גופים המפקחים, במישרין או בעקיפין, על חשיפת המשק לאיומי סייבר או תקיפות סייבר, מניעתם וההתמודדות איתם. לגופים אלו השפעה על הנעשה בתחום הסייבר בהיבטים שונים, החל מהגברת המודעות לחשיפות לסיכוני סייבר ועד לקביעת הוראות ביצוע לגופים שתחת פיקוחם. מבין הגופים האמורים, ניתן למנות מפקחים בתחום הפעילות הפיננסית כגון המפקח על הבנקים, רשות שוק ההון ביטוח וחיסכון, ורשות ניירות ערך.

ממשלת ישראל החליטה על מדיניות לאומית כוללת בתחום הגנת הסייבר במסגרת שורה של החלטות ממשלה, שבמרכזן הקמה של גוף לאומי חדש, מערך הסייבר הלאומי, להתמודדות עם תקיפות סייבר. מערך הסייבר הלאומי כולל גם את ה- CERT הלאומי, שלצדו פועל בשיתוף משרד האוצר גם מרכז הסייבר והרציפות הפיננסית.[1]

מסקירת ההתפתחויות שחלו בשנים האחרונות בשוק ההון בישראל נמצא, כי איומי סייבר הפכו לסיכון משמעותי ומוגבר עבור חברות במגוון ענפי משק ומעגל התאגידים שחוו תקיפת סייבר אחת או יותר הולך ומתרחב. לאור זאת, תהליך הערכת סיכוני סייבר וגילוי בנוגע לאירועי סייבר שחוו תאגידים כמו גם הטיפול בהם, הופכים להיות משמעותיים יותר לצורך הערכת כדאיות ההשקעה בניירות הערך של התאגידים המדווחים והבנת רמת הסיכון והחשיפה שלהם לאיומי סייבר.

[1] סגל הרשות מבקש להפנות את תשומת לב התאגידים המדווחים ל-'תורת ההגנה בסייבר לארגון' (הדפסה שניה) מאפריל 2018 ול-'תורת ההגנה בסייבר 2.0' מיולי 2021. המסמכים פותחו על-ידי מערך הסייבר הלאומי והם מהווים המלצות לכלל הארגונים במשק הישראלי. המסמך נכתב עבור דירקטוריונים והנהלות של חברות, מנהלי הגנה בסייבר ומיישמים וספקי IT וניתן להשתמש בהם לטובת העלאת החוסן בסייבר בארגון. קישור למסמך 2018. קישור למסמך 2021.

בנוסף, לאחרונה ביצעה מחלקת ביקורת והערכה ברשות ניירות ערך, ביקורת רוחב בנושא סיכוני סייבר בתאגידים מדווחים.[2] הביקורת נועדה לבחינת תהליך הערכת סיכוני סייבר, מתודולוגיית קביעת מהותיותם ואופן ניהולם בתאגידים המדווחים וכן בחינה של תהליך הגילוי והדיווח של התאגידים המדווחים בנוגע לסיכוני סייבר ואירועי סייבר.

ממצאי הביקורת הניבו את התובנות הבאות:

- **מעורבות הדירקטוריון בפיקוח על ניהול סיכוני סייבר** – קיימת חשיבות גדולה בקבלת עדכונים שוטפים מבעלי התפקידים הרלוונטיים בתאגיד ולמעורבות של הדירקטוריון ונושאי המשרה בתאגיד באיתור, ניהול ופיקוח של סיכוני סייבר ואבטחת מידע. מעורבות זו, תסייע בבניית מערך יעיל לניהול סיכונים ולתיאום בין היעדים העסקיים לבין המערך הטכנולוגי.
- **הערכת סיכוני סייבר וניהולם** – קיים ערך בביסוס מרכיבי ניהול סיכוני הסייבר בהתאם לכלים מקובלים, כגון: הערכת סיכונים באמצעות מתודולוגיה מקובלת דוגמת סקר סיכונים, קביעת תכנית עבודה שנתית/רב שנתית בתחום הסייבר וביצוע בקרות על ביצועה בפועל. בנוסף, קיימת חשיבות בהפעלת מערך אבטחת מידע תוך הסתייעות, במידת הצורך, בשירותי מיקור חוץ ומומחים בתחום אבטחת מידע וכן בביצוע בקרה על בחינת אופן הניהול של סיכוני סייבר באמצעות ביקורת פנים.
- **גילוי בנוגע לסיכוני סייבר ומתקפות סייבר** – יישום תהליך הערכת סיכונים סדור המבוסס על מתודולוגיה מקובלת דוגמת סקר סיכונים, מסייע לתאגיד להבטיח מתן גילוי נאות על סיכוני סייבר ואבטחת מידע כמו גם על גורמי סיכון אחרים הרלוונטיים לתאגיד. תהליך כאמור מאפשר בסיס לדיון בדירקטוריון בנוגע לגורמי הסיכון של התאגיד, דירוגם וגילוים בדוחות התקופתיים. לעניין זה, דירוג השפעת הסיכון מחייב התייחסות לסיכון השיורי לו חשוף התאגיד הלכה למעשה, בהתחשב בבקרות הקיימות ובמאפיינים הייחודיים של התאגיד ולא לסיכון השורשי (הסיכון הגולמי המובנה בהתעלם מהבקרות המופעלות להפחתת סיכון).
- **היערכות מוקדמת וגילוי על מתקפות סייבר בעת התרחשותן** – היערכות מוקדמת של התאגיד להתמודדות עם תקיפת סייבר, הכוללת הסדרה מראש של נהלים ותהליכי עבודה שיטתיים לטיפול ותגובה בנוגע לאירוע סייבר, וכן עיגון התהליכים הנדרשים לעניין גילוי ודיווח לציבור המשקיעים על התרחשות אירוע סייבר מהותי, יאפשרו לתאגידים לנהל ולהתמודד בצורה אפקטיבית יותר עם תקיפת סייבר בפועל ומתן הגילוי הנאות לציבור המשקיעים.

עמדת סגל זו מובאת לאור טיבם ומאפייניהם הייחודיים של סיכוני הסייבר - גודל הסיכון הפוטנציאלי, מערכות וגורמי הגנה שהנם בשלבי התהוות והתמקצעות, ההיקף ההולך וגדל של הגורמים המעוניינים לנצל את הסייבר ככלי עוין או כלי פשע, האפשרות להפעילו ממיקום חוץ טריטוריאלי ועוד. מטרת העמדה היא להגביר את מודעות התאגידים המדווחים לסיכון זה ולתת דגש להיבטים מסוימים אשר הגילוי לגביהם עשוי להידרש על פי הוראות דיני ניירות ערך. כמו כן, בעמדת הסגל הוטמעו, בין היתר, גם ממצאי ביקורת המתייחסים לדרישות הגילוי והדיווח אשר חלות על התאגידים המדווחים.

[2] ראו דוח ביקורת בנושא סייבר בקישור זה. יצוין כי בנוסף לביקורת הרוחב, מחלקת ביקורת והערכה ביצעה גם ביקורת פרטנית באחד התאגידים המדווחים ועיקרי ממצאיה מובאים בקישור זה.

אין בעמדה זו כדי ליצור חובות גילוי חדשות וכל גילוי בהתאם לעמדה זו כפוף למבחני המהותיות הרלוונטיים. כך למשל, תאגיד אינו נדרש לתאר סיכוני סייבר כלליים הקיימים ביחס לכלל המפוקחים, וזאת על מנת למנוע דיווחים גנריים (boilerplate) שמהותיות האמור בהם למשקיע שולית או לא קיימת, ו"תרומתם" מתמצה בהארכת הדיווחים ואף עלולה להקשות על הבנת הסיכון. התאגיד גם אינו נדרש למסור גילוי טכני ומפורט באופיו בענייני סייבר, אלא לנהוג בהקשר זה על פי דרישות ופרקטיקות הגילוי המקובלות גם בנושאים אחרים.

אין באמור לעיל כדי לגרוע מחובות גילוי העשויות לחול על התאגידים המדווחים מכוח הוראות דין אחרות.

ב. <u>מונחים</u>

להלן מונחים שישמשו בהמשך עמדה זו[3]:

"**איום סייבר**" או "**סיכון סייבר**" - סיכון להתרחשות תקיפת סייבר;

"**הגנת סייבר**" - מכלול הפעולות הנדרשות למניעה, להתמודדות ולטיפול בתקיפת סייבר או איום סייבר, לצמצום השפעתם והנזק הנגרם מהם, במהלכם ואחריהם, ובכלל זה פעולות אבטחת מידע;

"**תקיפת סייבר**" או "**אירוע סייבר**" – תקיפה במרחב הסייבר או פעילות אחרת אשר נועדה לסכן נכסי סייבר או מערכות ותשתיות הנתמכות על ידם.

ג. <u>הדרישות הקיימות בדין באשר לסיכוני הסייבר ולמקרים של התממשותם</u>

קיימות בדין דרישות גילוי שונות באשר לגורמי סיכון או להתממשותם. להלן העיקריות שבהן[4]:

1. <u>גילוי בתשקיף ובדו"ח התקופתי</u>

א. <u>גילוי על גורמי סיכון</u>

סעיף 39 לתוספת הראשונה לתקנות ניירות ערך (פרטי התשקיף וטיוטת התשקיף – מבנה וצורה), התשכ"ט – 1969 (להלן: "**התוספת הראשונה**") מסדיר בין היתר את חובות הגילוי ביחס לגורמי הסיכון של התאגיד, כדלקמן:

> "**39. דיון בגורמי סיכון**
>
> (א) יובא סיכום קצר של האיומים, 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.

---

[3] המונחים לקוחים מתזכיר חוק הגנת הסייבר ומערך הסייבר הלאומי, התשע"ח – 2018 בהתאמות מסוימות (בעיקר הוספת המונח "סיכון סייבר" כמונח חלופי למונח "איום סייבר". חוק ניירות ערך עושה שימוש במונח "סיכון" ולא במונח "איום" ולפיכך היה צורך בכך).

[4] כאמור מדובר בדרישות גילוי עיקריות שאין בהן כדי למצות את מלוא חובות הדיווח החלות בקשר עם סיכוני סייבר. כך למשל, תאגיד שנפגע בתקיפת סייבר באופן שבנוסף לנזקים האחרים, האירוע השפיע מהותית על התקשרויות עם לקוחות מהותיים, יתייחס לאמור במסגרת סעיף הלקוחות בפרק תיאור עסקי התאגיד. דוגמה נוספת, כאשר על תאגיד חלה רגולציה ייעודית בנושא סייבר, המשפיעה עליו באופן מהותי, עליו להתייחס לאמור במסגרת סעיף מגבלות ופיקוח על פעילות התאגיד בפרק תיאור עסקי התאגיד. דוגמא אחרת הנה להתייחס לנאותות היקף הביטוח היכן שרלוונטי.

(ב) 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."

סיכוני סייבר הם גורם סיכון ככל סיכון אחר. אם קיים בתאגיד סיכון סייבר מהותי הרלוונטי לפעילותו, על הגילוי בדבר סיכון זה לכלול תיאור בעניינו, התייחסות לקיומה של מדיניות הגנה ובדיקת האפקטיביות שלה.

כאשר תאגיד בוחן את מהותיות סיכוני הסייבר, <u>רצוי לשקול בין היתר את הגורמים הבאים</u>:

- התרחשות תקיפות סייבר קודמות, לרבות חומרתן ותדירותן;
- ההסתברות להתרחשות תקיפות סייבר;
- אפקטיביות יכולות התאגיד למנוע או להקטין את החשיפה לסיכוני הסייבר;
- היבטים עסקיים של התאגיד ופעילותו, היוצרים סיכונים מהותיים בתחום הסייבר, והעלויות וההשלכות הפוטנציאליות של סיכונים אלה, לרבות סיכונים ספציפיים לתחום פעילותו וסיכונים של ספקי שירות וצדדים שלישיים אחרים עימם התאגיד בא במגע;
- המשאבים הכרוכים בשמירה על הגנות סייבר לרבות קיומו של כיסוי ביטוחי המתייחס לתקיפות סייבר;
- הפוטנציאל לפגיעה בנכסים ובכללם קנין רוחני ומוניטין, וכן עוצמת הפגיעה האפשרית ביתרונות תחרותיים שיש לתאגיד;
- חוקים ותקנות קיימים או תלויים ועומדים, אשר עשויים להשפיע על העלויות הנלוות לתאגיד בקשר עם אותה רגולציה.

ב. <u>גילוי על מדיניות ניהול סיכוני סייבר ואבטחת מידע</u>

היערכות מוקדמת של התאגיד להתמודדות עם סיכון הסייבר בכלל ועם תקיפת סייבר בפרט וקביעת מדיניות לניהול הסיכון, עשויות להקל על התנהלות התאגיד בעת משבר. בהתאם, אם קיים בתאגיד סיכון סייבר מהותי הרלוונטי לפעילותו, על התאגיד:

- לפרט את אסטרטגיית ניהול הסיכונים בנושא, הכוללת את <u>מדיניות ניהול הסיכון</u>, מתודולוגיות, נהלים, תהליכי עבודה, פעולות ובקרות לשם ניהול והתמודדות עם סיכון הסייבר בתאגיד ואת הערכתו בדבר <u>אפקטיביות</u> מדיניות ניהול הסיכונים בהתמודדות והפחתת סיכון הסייבר.
- לציין אילו משאבים מוקצים על ידו לניהול סיכוני סייבר, ובפרט זהות הגורם המאשר את מדיניות ניהול סיכון הסייבר בתאגיד, בעל התפקיד בתאגיד אשר אחראי ליישום המדיניות, ככל שקיימת, הגדרת תפקידו ולמי הוא כפוף בתאגיד. ככל שמדובר בשירותי מיקור חוץ יש לציין זאת ולפרט את מהות השירותים שמתקבלים.

ג. <u>גילוי על מומחיות נושאי משרה וחברי דירקטוריון בתחום הסייבר</u>

לדירקטוריון התאגיד תפקיד חיוני בכל הנוגע לפיקוח והשפעה על התוויית ותפעול מערך ניהול סיכוני סייבר יעיל ומיקסום התיאום בין היעדים והצרכים העסקיים לבין המערך הטכנולוגי. הנהלת התאגיד היא הגורם אשר מנהל ומיישם בפועל את מדיניות ניהול הסיכונים. על כן, קיימת

חשיבות לקיומם של תקשורת, תיאום ושיתוף פעולה הדוק בין הדירקטוריון לבין ההנהלה הבכירה בנוגע לזיהוי הסיכון והערכתו, ניהול הסיכון וקיום בקרות שוטפות.

- על כן, במסגרת מתן מידע על השכלתם ועיסוקם של הדירקטורים ונושאי המשרה ב-5 השנים האחרונות, כנדרש בתקנה 26(א)(9) ו- 26א(5) לתקנות ניירות ערך (דוחות תקופתיים ומיידיים), תש"ל-1970 (להלן: "**תקנות הדוחות**"), אם לנושא המשרה בתאגיד יש ניסיון, מומחיות או מיומנות בנושא אבטחת מידע או סייבר, על התאגיד לציין עובדה זו ולפרטה.
- יצוין בזאת, כי על אף היתרונות בידע ובמיומנות של חברי הדירקטוריון ונושאי המשרה בתחום הסייבר, בפני התאגיד פתוחות אפשרויות נוספות לקבלת סיוע מקצועי נדרש בנושא הסייבר ובכלל זה האפשרות להיוועץ עם מומחים חיצוניים במידת הצורך. בהתאם, אם בחר התאגיד להשתמש בשירותי מיקור חוץ ובמומחים חיצוניים, עליו לפרט שימוש בסיוע כאמור כחלק ממדיניות ניהול הסיכון.

ד. <u>גילוי על אירועים החורגים מעסקי התאגידים הרגילים</u>

סעיף 36 לתוספת הראשונה לתקנות פרטי תשקיף מסדיר את חובות הגילוי במקרה של אירוע או ענין החורגים מעסקי התאגיד הרגילים:

"**36. אירוע או ענין החורגים מעסקי התאגיד הרגילים**

יובאו פרטים בדבר כל אירוע או ענין, ... , החורגים ממהלך העסקים הרגיל של התאגיד בשל טיבם, היקפם או תוצאתם האפשרית, ואשר יש להם או עשויה להיות להם השפעה מהותית על התאגיד."

במקרה של תקיפות סייבר מהותיות בתקופת הדוח, על התאגיד לבחון תיאור תמציתי של עיקרי האירועים שהתרחשו בתקופת הדוח או הכללה על דרך הפניה של דוחות מיידיים שפרסם התאגיד שבמסגרתם נכלל תיאור אודות האירועים כאמור. אם פורסם דוח מיידי על אירוע סייבר, על התאגיד לבחון האם התגלה מידע מהותי נוסף בנוגע לאירוע ולפרטו במסגרת הדוח התקופתי. מידע נוסף כאמור יכול שיכלול השפעות על המצב הפיננסי של התאגיד, שינוי במדיניות החברה בעקבות האירוע וכיוצא בזה.

התיאור יכלול, בהתאם לנסיבות ולעובדות ולמיטב ידיעת התאגיד, פרטים כגון – זהות או סוג התוקפים, נסיבות התקיפה, כמות התקיפות ומשך זמן התקיפה, האם להערכת התאגיד היא הסתיימה, היקף וסוג הנזק שאירע לרבות השלכות עקיפות, הערכת התאגיד האם אותר מלוא הנזק הישיר, התמודדות התאגיד עם התקיפה, הפקת לקחים והאמצעים שננקטו כדי למנוע תקיפה חוזרת מסוג זה ועוד. אף אם לא קיים אירוע בודד מהותי אך התאגיד חווה מספר אירועים אשר במקובץ הם מהותיים, נדרש לבחון גילוי כאמור.

תקנה 8א לתקנות הדוחות קובעת כי תיאור התאגיד והתפתחות עסקיו במסגרת הדו"ח התקופתי יובא בהתאם לפרטים ולעקרונות של התוספת הראשונה[5]. לפיכך כוחן של הוראות הגילוי לעיל יפה גם לדוח התקופתי.

---

[5] תקנה 8א לתקנות הדוחות:

"**תיאור עסקי התאגיד**

בדוח התקופתי יובאו תיאור התאגיד והתפתחות עסקיו כפי שחלו בשנה האחרונה, בהתאם לפרטים ולעקרונות שבתוספת הראשונה לתקנות פרטי תשקיף, בשינויים המחויבים ובכל מקום בתוספת שבו נאמר "תשקיף", ייקרא - דוח."

2. גילוי בדו"ח הדירקטוריון

מצב ענייני התאגיד - תקנה 10 לתקנות הדוחות מסדירה את ההתייחסות למצב ענייני התאגיד בדו"ח הדירקטוריון, וקובעת כדלקמן:

"10. דו"ח הדירקטוריון על מצב עניני התאגיד

(א) יובא דו"ח הדירקטוריון על מצב עניני התאגיד בשנת הדיווח ובו הסברים של הדירקטוריון על מצב עסקי התאגיד, תוצאות פעולותיו, הונו העצמי ותזרימי המזומנים שלו; ההסברים יתייחסו לאופן השפעתם של אירועים על הנתונים שבדו"חות הכספיים ועל הנתונים שבתיאור עסקי התאגיד, אם השפעה זו מהותית, ולסיבות שהביאו לשינויים שחלו במצב עניני התאגיד בהשוואה לשנות הדיווח הכלולות בדו"חות הכספיים; דו"ח הדירקטוריון יתייחס לנתונים העיקריים המצויים בדוחות הכספיים ובמסגרת תיאור עסקי התאגיד, ויכלול מידע נוסף המצוי בידי התאגיד לגבי שנת הדיווח, והכל אם לדעת הדירקטוריון הם חשובים להבנת מצב עניני התאגיד באופן מאוזן בידי משקיע סביר השוקל קניה או מכירה של ניירות הערך של התאגיד. דוח הדירקטוריון יכלול גם פרטים נוספים כמפורט בתקנה זו."

השפעת גורמים חיצוניים - סעיף 6 בתוספת הראשונה לתקנות הדוחות מסדיר את העניינים אליהם יש להתייחס בדו"ח הדירקטוריון, וקובע כדלקמן:

"6. השפעת גורמים חיצוניים

יוסברו נתונים מהותיים מאוד שהופיעו במסגרת תיאור עסקי התאגיד בהתאם לתקנה 8א לתקנות העיקריות ושלא ניתן להם הסבר במסגרת סעיפים 2 עד 5."

ככל שסבור תאגיד שחשיפתו לסיכוני סייבר הפכה בשנת הדוח למהותית יותר להבנת פעילותו באופן כללי, או אם אירעו תקיפה או תקיפות סייבר בעלות השפעה מהותית על אחד או יותר מסעיפי הדוחות הכספיים (מאזני או תוצאתי), יובאו הסברי הדירקטוריון בענין זה. הסברי הדירקטוריון ייתכן ויידרשו אף אם אין לאירוע השפעה ישירה על הדוחות הכספיים אך פרטי האירוע תוארו כחלק מתיאור עסקי התאגיד בהתאם לתקנה 8א לתקנות הדוחות. כך למשל, אם תאגיד רכש ביטוח סייבר.

במסגרת ההסברים תינתן התייחסות להשפעת האירועים על סעיפים מהדוחות הכספיים שהושפעו מהותית בשל סיכוני סייבר או תקיפות סייבר, ככל שמדובר בהשפעה מהותית, כגון:

- השפעות על סעיפים מאזניים כדוגמת לקוחות, מלאי, רכוש בלתי מוחשי (כגון קנין רוחני, מוניטין וכדומה).
- השפעות על סעיפים תוצאתיים כדוגמת אובדן הכנסות, ירידות ערך, הפרשות, פגיעה ברווחיות.
- סך העלויות שנוצרו לתאגיד הנובעות מהיערכות בגין הגנת סייבר.
- השפעת תקיפה או תקיפות סייבר אשר טרם קיבלו או לא יקבלו ביטוי במסגרת הדוחות הכספיים אך הם מהותיים לפעילות התאגיד, למשל – הגשת תביעות, פגיעה בפיתוח מוצר של התאגיד או פעילות אחרת שלו, פגיעה בתיק הלקוחות, פגיעה במוניטין או ביתרונות תחרותיים וכו'.

3. גילוי בדיווחים מיידיים

תקנה 36(א) לתקנות הדוחות עניינה "אירוע או ענין החורגים מעסקי התאגיד הרגילים" והיא קובעת כדלקמן:

" 36. אירוע או ענין החורגים מעסקי התאגיד הרגילים

בדוח יובאו פרטים בדבר כל אירוע או ענין החורגים מעסקי התאגיד הרגילים בשל טיבם, היקפם או תוצאתם האפשרית ואשר יש להם או עשויה להיות להם השפעה מהותית על התאגיד, וכן בדבר כל אירוע או ענין שיש בהם כדי להשפיע באופן משמעותי על מחיר ניירות הערך של התאגיד."

בהתאם, בקרות תקיפת סייבר והבחינה של מהותיות האירוע ובהתאם אם אירוע זה מחייב פרסום דוח מיידי, תאגיד נדרש, בין היתר, לשקלל את מכלול הנזק ופוטנציאל הנזק שנגרם/ עלול להיגרם כתוצאה מהתקיפה, הן במישרין והן בעקיפין. בנוסף, מהותיות של אירוע צריכה להיבחן הן בהתאם לפרמטרים כמותיים והן בהתאם לפרמטרים איכותיים. על כן, יתכן שאירוע ייחשב כמהותי ובהתאם מחייב דיווח מיידי גם במקרים בהם מחד לא צפוי נזק כספי ממשי לתוצאות התפעוליות של התאגיד, אך מאידך קיימת השפעה מהותית על התאגיד במישור האיכותי.

<u>להלן מספר דוגמאות, לא ממצות, לאירועים או עניינים בתחום הסייבר, אשר עשויים לחייב פרסום דיווח מיידי מכוח תקנה 36</u>:

- פעילותו העסקית של תאגיד הושבתה באופן מלא או חלקי לפרק זמן;
- מאגרי מידע נפרצו באופן אשר עלול להשפיע באופן מהותי על פעילות התאגיד במישרין או בעקיפין. ככל שהמאגר מוגן ע"י דיני הגנת הפרטיות יש להתייחס לכך בנפרד ובנוסף;
- מערכת מחשוב של התאגיד, המהותית לפעילותו, ניזוקה באופן הפוגע מהותית בפעילות התאגיד;
- התאגיד נדרש לשלם או מעריך כי יידרש לשלם כופר בסכום מהותי בעקבות תקיפת סייבר;
- תאגיד גילה כי גורמים עוינים "צותתו" למערכות המחשוב (כגון דואר אלקטרוני), ונחשפו לסודות עסקיים או למידע רגיש אחר או אם גילה כי נגנב מידע עסקי שחשיפתו עלולה לפגוע מהותית בתאגיד.
- במוצרי החברה או במערכות שהחברה בנתה או הייתה אחראית להן התגלתה פרצת אבטחה מתחום הסייבר שבגינה קיימת לחברה חשיפה מהותית (כיצרנית, כספקית המוצר וכד');

למען הסר ספק, מקום שקמה לתאגיד חובת דיווח מיידי מכח תקנה 36 לתקנות הדוחות בקשר עם איומי או תקיפות סייבר, הרי שקיימת לו גם הזכות לעכב דיווח בהתאם לקבוע בתקנה 36(ב) לתקנות הדוחות ובפרט כאשר פרסום הדיווח עלול למנוע השלמת פעולה של תאגיד כקבוע בהוראות תקנה 36(ב1)(2) לתקנות הדוחות. יובהר כי בהתאם להוראות תקנה 36(ב) ו- 36(ב1)(ד), זכות העיכוב פוקעת אם המידע בדבר האירוע פורסם ברבים.

בדיווח מכוח תקנה 36(א) לתקנות הדוחות יכלול תאגיד כל פרט חשוב להערכת השלכות האירוע המדווח על עסקי התאגיד, ובכלל זה –

א. **תיאור האירוע** – על התאגיד לכלול מידע בקשר עם מועד תחילת האירוע ומועד סיומו, מה כלל האירוע, סוג הנתונים שנחשפו, הגורמים שהביאו לקרות האירוע וצעדים שננקטו בעניינו.

ב. **תיאור הנזק והערכת הנזק** – על התאגיד להתייחס לתיאור הנזק והערכת הנזק. במסגרת זו על התאגיד להביא בחשבון את הצורך לתת ביטוי, בין היתר, לעניינים הבאים – הפעילויות והנכסים שהושפעו מהאירוע והערכת הפגיעה בהם, השפעה אפשרית על תוצאות פעילות התאגיד ובכלל זה פגיעה אפשרית בהכנסות, מידת הפגיעה (ככל שישנה) ביחסי לקוחות או ספקים, או פגיעה במוניטין של התאגיד. עד כמה שניתן, על התאגיד לכלול התייחסות להערכה כוללת של הנזק הצפוי.

ג. **דיווחים משלימים על האירוע** – יתכנו מקרים בהם פרטים מסוימים כגון, היקף החשיפה או הנזק, יתבררו במועד מאוחר למועד האירוע. כך למשל, ייתכנו פגיעה מאוחרת או נמשכת בנכסים, חשיפות לתביעות משפטיות, עלויות מהותיות להקמת מערכות הגנה חדשות וכדומה. על התאגיד לבחון את הצורך בגילוי משלים על האירוע והתפתחויות מאוחרות לו בין היתר בהתאם להוראות תקנה 37(א)(2) לתקנות הדוחות.

****