

דוח ריכוז ממצאי ביקורת רוחב
בנושא סיכוני סייבר בתאגיד מדווח
ינואר 2023
מיועד לתאגידים מדווחים

רקע

איומי סייבר הפכו בשנים האחרונות לסיכון משמעותי עבור חברות במגוון ענפי משק. מספר לא מבוטל של חברות סבלו מהתקפות סייבר אשר גרמו להשבתת פעילותן, נזקים כספיים ישירים ונזקי מוניטין ארוכי טווח. המעגל המתרחב של חברות המושפעות ממתקפות סייבר, כולל גם תאגידים מדווחים אשר חוו מתקפות בעלות השפעה מהותית יותר מבעבר על פעילותם העסקית השוטפת. לאור זאת, הערכה וגילוי ביחס לסיכוני סייבר וכן גילוי בנוגע לתקיפות סייבר שחוו חברות והטיפול בהן, הופכים להיות משמעותיים יותר עבור משקיעים לצורך הערכת כדאיות ההשקעות בניירות ערך של החברות והבנת רמת הסיכון והחשיפה שלהן למתקפות סייבר.

באוקטובר 2018, פרסמה מחלקת תאגידים ברשות ניירות ערך עמדה משפטית מס' 33-105 בעניין "גילוי בנושא סייבר" (להלן: "העמדה המשפטית") אשר מטרתה הייתה העלאת מודעות התאגידים המדווחים לסיכוני סייבר, תוך מתן דגשים להיבטים מסוימים אשר הגילוי לגביהם עשוי להידרש על פי הוראות דיני ניירות ערך. יצוין כי בימים אלו מפרסם סגל מחלקת תאגידים עדכון לעמדה המשפטית, אשר במסגרתו יכללו הבהרות ודגשים לעמדה וכן יינתן ביטוי לחלק מהתובנות אשר יוצגו במסמך זה¹.

נושאי הביקורת

במהלך שנת 2022 ביצעה מחלקת ביקורת והערכה ברשות (להלן: "מחלקת הביקורת") ביקורת רוחב במטרה לבחון את תהליך הגילוי והדיווח של תאגידים מדווחים בכל הקשור לסיכוני סייבר ותקיפות סייבר (להלן: "הביקורת"). הנושאים שנבחנו במסגרת הביקורת הינם כדלהלן:

1. המתודולוגיה בה השתמשו תאגידים לבחינת מהותיות סיכון הסייבר ובחינת סבירותה, וכן בחינת האופן בו בחנו התאגידים את הצורך במתן גילוי למשקיעים ביחס לסיכוני סייבר ועוצמתם, בהתאם לכך.
2. אופי הגילוי הנוגע למדיניות/ מנגנוני ההגנה בהם נקטו תאגידים לצורך הפחתת סיכון הסייבר, פיקוח על יישומה של מדיניות זו ובדיקת האפקטיביות שלה.
3. היבטים בניהול סיכוני הסייבר על ידי חברות המדגם, לרבות כלים להפחתת חשיפות.

¹ [העמדה המשפטית](#)

4. מתן גילוי על תקיפות סייבר שחוו תאגידיים, לרבות בחינת תהליכי קבלת ההחלטות בנוגע למהותיות המתקפות לצורך החלטה בדבר נחיצות הגילוי, טיב הגילוי שניתן וכדומה.
5. אופן הטיפול בתקיפות סייבר לאחר התרחשותן ובהתאמה בחינת הגילוי שניתן לציבור על אופן הטיפול, תוצאותיו והשלכותיו על התאגיד, לרבות צעדי התיקון שנקטו בעקבות המתקפה והאם השפיע או צפוי להשפיע על האסטרטגייה העסקית/ תוצאות הפעילות/ מצבה הפיננסי של החברה.

שיטת הביקורת והיקפה

הביקורת בוצעה באמצעות ניתוח מענה לשאלון רוחב (להלן: "השאלון") אשר הופץ בקרב מדגם של 72 תאגידיים מדווחים המשתייכים למגוון ענפי בורסה (להלן: "החברות" או "חברות המדגם"). השאלון כלל 24 שאלות, כאשר החברות התבקשו לספק אסמכתאות התומכות במענה שלהן לחלק משאלות אלו.

יודגש כי מדגם החברות שנבחר עבור הביקורת אינו מדגם מייצג של כלל החברות הציבוריות וכל ענפי הפעילות בשוק ההון. הביקורת בחרה להתמקד במדגם חברות ממספר סקטורים אשר מבחינה ראשונית של הסביבה העסקית בהן הן פועלות, נראה שאופי פעילותן ו/או המידע שקיים במאגריהן עשוי לשקף היתכנות לחשיפה מוגברת לסיכון סייבר, וזאת מתוך מטרה של בחינה והסקת מסקנות מהתנהלות של קבוצת חברות בעלת פוטנציאל גבוה יותר לקיומו של הסיכון. לצורך כך, כאמור, נבחרו לצורך המדגם חברות מתחומי פעילות אשר להערכתנו פוטנציאל הנזק שעלול להיגרם כתוצאה מהשבתת פעילותן או כתוצאה מדליפת מידע רגיש ממאגריהן עשוי להיות גבוה יותר, וכן חברות אשר לא כללו בדוחותיהן התקופתיים את סיכון הסייבר כסיכון אשר יש לו השפעה על החברה או שחל אצלו שינוי מהותי בדירוג סיכון זה במהלך השנתיים האחרונות, וכן חברות אשר דירוג השפעת סיכון הסייבר על פעילותן חריג מהממוצע בענף הפעילות אליו הן משתייכות.

יש לציין כי במדגם החברות לא נכללו חברות ברישום כפול או חברות שיש להן רגולטור מאסדר בנושא הסייבר (כגון בנקים, ביטוח, בתי השקעות, חברות תקשורת וכו'). כמו כן, אין ללמוד מבחירת חברות המדגם ומהסקטורים שנסקרו, כי החברות הנבחרות הן בהכרח בעלות סיכון סייבר מוגבר ביחס לחברות אשר לא נבחרו במדגם או כי סקטורים שלא נבחנו אינם בעלי סיכון סייבר מהותי. על כל תאגיד בכל סקטור פעילות בשוק ההון לבחון את סיכוני הסייבר שחלים עליו בהתאם לנסיבותיו הספציפיות, ובכלל זאת, רמת אבטחת המידע שלו, המשאבים שמוקצים על ידו להגנת סייבר, מומחיות כוח האדם בתאגיד בנושא, חשיפת ענף הפעילות אליו משויך התאגיד לפגיעה אפשרית בנכסי סייבר ובתשתיות הנתמכות על ידם, אפקטיביות מדיניות ניהול סיכוני הסייבר וכיוצא בזה.

דוח ריכוז הממצאים שלפניכם נועד לשקף את עמדת סגל הרשות במספר סוגיות אשר התגבשו במהלך הביקורת, ויפורטו להלן. על התאגידיים המדווחים לבחון את הצורך בהתאמתן של התובנות המוצגות בדוח זה לפעילותם, ובמידת הצורך לשקול לעגן את הפרקטיקות המפורטות בו כחלק מתהליכי העבודה הנוהגים אצלם.

ממצאי הביקורת ועמדות סגל הרשות לגביהם

1. ניהול סיכוני אבטחת מידע וסייבר

ניהול סיכוני סייבר מהווה נדבך חשוב במסגרת ניהול הסיכונים הכולל של חברה, בין השאר במטרה לאפשר רציפות תפקודית מבחינה עסקית ולתמוך בהשגת יעדיה העסקיים של החברה. ניהול סיכונים אפקטיבי מורכב בדרך כלל מכמה רכיבים עיקריים: זיהוי הסיכון, הערכת הסיכון, ניתוח גורמי הסיכון, ניהול הסיכון, בקרה וניטור שוטפים. בשל ייחודיותו של סיכון הסייבר, הגנה על ארגון מפני איומי סייבר דורשת ידע רב והתמחויות שונות ומגוונות כגון התמחויות טכנולוגיות, ארגוניות ותהליכיות. לצורך מקסום תהליכי הערכת סיכון הסייבר בארגון וניהולו, נדרש תיאום ושיתוף פעולה הדוק בין הצד העסקי בארגון לצד הטכנולוגי.

1.1. מעורבות דירקטוריון בפיקוח על ניהול סיכוני סייבר

לדירקטוריון חברה תפקיד חשוב כגוף המפקח על פעילותה התקינה, לרבות פעילותה בתחום ניהול סיכוני סייבר. הצורך בידע ומיומנות טכנולוגית של חברי דירקטוריון והנהלה התחזק במיוחד בשנים האחרונות, לאור נגיעת התחום הטכנולוגי בנדבכים עסקיים רבים של חברות.

תוצאות ניתוח מענה חברות המדגם בהקשרים אלו מצביעות על מעורבות מעטה יחסית של הדירקטוריון בכל הקשור לפיקוח על היבטי הגנה מפני סיכוני סייבר ולאופן ניהול סיכוני אבטחת מידע בכלל. כך למשל, בכ-90% מחברות המדגם, נוהל אבטחת מידע לא אושר כלל על ידי דירקטוריון החברה.

ממצא נוסף מצביע על כך שחברי הדירקטוריון של כ-70% מחברות המדגם אינם מקבלים דיווחים עיתיים הנוגעים לסטטוס הגנת הסייבר ואבטחת המידע בחברה, ואינם מקיימים דיונים בנושאים הרלוונטיים לתחום זה. בנוסף, בחלק מהחברות לא מתקיימים כלל דיונים בדירקטוריון בכל הנוגע להשפעת סיכוני סייבר על פעילותה העסקית של החברה. עוד יצוין כי חלק ניכר מהחברות אשר כן מקיימות דיונים בדירקטוריון בהקשר זה, אינן עושות זאת באופן עיתי וסדיר, אלא בהתאם לצורך בלבד.

עמדת סגל הרשות היא כי קיימת חשיבות גדולה במעורבות של דירקטוריון בפיקוח על בנייה ותפעול של מערך ניהול סיכוני סייבר יעיל. ללא מעורבות דרגים בכירים, תוגבל היכולת לבצע תיאום אפקטיבי בין היעדים והצרכים העסקיים של הארגון ובין המערך הטכנולוגי שלו. מעבר לכך, למעורבות זו השפעה לא מבוטלת על התרבות הארגונית של החברה והתנהלות עובדיה במרחב הקיברנטי.

מעורבות דירקטוריון יכולה לבוא לידי ביטוי בהעלאת נושא הסייבר באופן עיתי על סדר היום של דיוני הדירקטוריון, כאשר במסגרת זו יתקבלו, בין היתר, דיווחים שוטפים בנושא מאנשי הטכנולוגיה בחברה, יינתנו אישורים להתקשרויות עם מיקור חוץ בתחום, ידונו בהשפעת סיכוני סייבר על פעילות התאגיד ויתקבלו עדכונים ויעוץ ממומחים חיצוניים במקרה הצורך. במסגרת דיונים אלו ניתן, בין היתר, להתייחס להיערכות החברה להתמודדות עם מתקפת סייבר, ניסיונם ומומחיותם של בעלי תפקידים המנהלים תחום זה בחברה, ביצוע עדכונים תוכנה רלוונטיים נדרשים, אופן העלאת מודעות עובדי

החברה לסיכוני סייבר וכדומה. מידע עיתי זה יהווה בקרה יעילה על הנעשה בחברה בתחום זה, ואף יאפשר לשדר מסרים על חשיבות הנושא לעובדי החברה ובכך לפתח "חשיבת סייבר" ארגונית.

יצוין כי אחת הסיבות האפשריות לחוסר מעורבות של דירקטוריון בכל הקשור לניהול סיכוני סייבר, עשויה להיות היעדרם של בעלי ידע או מומחיות בתחום אבטחת מידע או סייבר בקרב חבריו, כפי שעלה ממרבית החברות שנדגמו. יודגש כי קיומה של מומחיות בתחומים אלו אינה ערובה בלעדית לניהול אפקטיבי יותר של סיכוני סייבר, וכי שימוש בחלופות ראויות כגון היוועצות עם מומחים חיצוניים² וכדומה, עשוי להגשים את אותה מטרה.

בהקשר זה מוצע כי הדירקטוריון יבחן את מידת נחיצותה והיקפה של המומחיות הטכנולוגית הנדרשת לצורך מילוי תפקידיו כראוי, לרבות הצורך במינוי דירקטור בעל מומחיות מסוג זה, וזאת בכפוף למאפייניה של החברה, אופי פעילותה, סיכוני סייבר ואבטחת מידע המוטלים לפתחה וכדומה.

1.2. מערך אבטחת מידע

מרכיב חשוב בניהול סיכוני סייבר בחברה הוא קיום מערך אבטחת מידע אפקטיבי. מערך זה יכול להיות מופעל באופן עצמאי על ידי פונקציות בחברה, באמצעות מיקור חוץ או בשילוב של שניהם, הכל בהתאם לצרכיה העסקיים של החברה. אפקטיביות מערך אבטחת המידע עשויה להתקבל מתיאום ושיתוף פעולה בין המערך, המורכב לרוב מאנשי טכנולוגיה, לבין הצד העסקי בחברה. כמו כן, מצופה כי הצעדים הננקטים לצורך ניהול סיכוני הסייבר, יבוקרו על ידי דרגים בכירים בחברה.

מתוצאות ניתוח מענה החברות לשאלון עולה, כי מרביתן המכריע של החברות מפעילות מערך אבטחת מידע, כאשר במחצית מהחברות מדובר במערך עצמאי. עוד עולה ממענה החברות כי המערכים העצמאיים מנוהלים בעיקר על ידי מנהלי מערכות מידע ואנשי טכנולוגיה, כאשר רק במספר חברות מצומצם קיימים אורגנים נוספים הקשורים למערך, כדוגמת ועדת היגוי המורכבת מגורמים עסקיים וטכנולוגיים כאחד.

מבחינת שיטת העבודה של מערכי אבטחת המידע נמצא, כי רק אצל כמחצית מחברות המדגם קיימת תכנית עבודה שנתית מסודרת, כאשר במחצית מאלו קיימת גם בקרה אחר ביצוע תכנית העבודה על ידי דרגים בכירים בחברה הלכה למעשה (כדוגמת ועדת היגוי, ועדת אבטחת מידע, מנכ"ל, מנמ"ר ראשי וכדומה).

היבט נוסף בעניין אפקטיביות המערך נוגע למתודולוגיה של ניהול סיכוני סייבר. לאורך השנים ובמיוחד בשנים האחרונות, פותחו בארץ ובעולם מספר תקנים שמטרתם סיוע בבניית מערכי ניהול סיכוני סייבר באופן יעיל, תוך התאמה למאפייניה וצרכיה של כל חברה וחברה. יודגש כי יישום תקנים והטמעת נהלי עבודה אינם בגדר חובה על פי הוראות הדין, אך לצורך ניהול אפקטיבי של גורמי הסיכון בחברה, קיים ערך רב ביישומם. תוצאות ניתוח

² סעיף 266(א) לחוק החברות, התשנ"ט-1999.

מענה חברות המדגם מצביעות על היעדר יישום מתודולוגיה סדורה בקרב החברות בכל הקשור לניהול אבטחת מידע וסיכוני סייבר, כאשר כ-83% ממערכי אבטחת המידע בחברות אינם מיישמים אף לא אחד מהתקנים המקובלים בתחום אבטחת המידע או הסייבר.

עוד עולה כי חלק מהחברות אשר מערך אבטחת המידע שלהן מבוסס ברמה זו או אחרת על מיקור חוץ, אינן מאשרות התקשרויות אלו על ידי הנהלת החברה או הדירקטוריון שלה.

סגל הרשות מפנה בהקשר זה להמלצתו בסעיף 1.1 לעיל בדבר חשיבות מעורבותו של הדירקטוריון בבנייתו ותפעולו של מערך יעיל לעניין ניהול סיכוני סייבר, ובין היתר לצרכי תיאום בין היעדים והצרכים העסקיים של הארגון ובין המערך הטכנולוגי שלו. בהקשר זה אף מוצע כי נושאים כגון תוצאות הערכת סיכוני הסייבר והתקשרויות עם מיקור חוץ בתחום זה, יובאו בפני דירקטוריון החברה.

כמו כן, על מנת שמערך אבטחת המידע יפעל באופן אפקטיבי בהתמודדותו עם איומי הסייבר המשתנים בקצב מהיר בשנים האחרונות, מומלץ כי יפעל בהתבסס על תכנית עבודה שנתית/ רב שנתית בתחום הסייבר וכן כי ביצוע ויישום תכנית העבודה הלכה למעשה יבוקר על ידי דרגים בכירים בחברה.

בנוסף, לצורך ניהול אפקטיבי יותר של סיכוני הסייבר, מומלץ לחברות לשקול יישומו של אחד מהתקנים המקובלים בתחום הסייבר. יצוין כי ברוב התקנים ניתן לבצע התאמה לגודל החברה וצרכיה העסקיים.

1.3. הערכת סיכוני סייבר וניהולם

בשל העובדה שאיומי סייבר הפכו כאמור לנפוצים יותר, ובמקביל דרישות הרגולציה החריפו בהתאמה (תקנות הגנת הפרטיות לדוגמה), הפכה הערכת סיכוני הסייבר לתהליך שהינו בגדר חובה עבור כל ארגון, כאשר במסגרתה נבדקים מערכי האבטחה של הארגון, רמת מוגנותו, פירצות האבטחה הקיימות וכדומה. מטרת הערכת הסיכונים היא בדיקת רמות האבטחה הקיימות במסגרת התהליכים והמערכות של הארגון, מאבטחת מידע פיזית ועד לאבטחת התשתיות, לרבות אתרי האינטרנט של הארגון, מערכות הפעלה, רשתות, מאגרי מידע, ניהול משתמשים והרשאות, תהליכי גיבוי ועוד.

מניתוח מענה חברות המדגם לשאלון עולה, כי כ-40% מהחברות לא ביצעו הערכת סיכוני סייבר בשלוש השנים האחרונות. עוד יצוין כי כמעט מחצית מהחברות אשר כן ביצעו לפחות הערכת סיכוני סייבר אחת בשלוש השנים האחרונות, לא הציגו את תוצאות הערכת הסיכונים במסגרת ישיבות הדירקטוריון, עובדה אשר יש בה כדי לחזק ממצאים קודמים שהוצגו לעיל לעניין מעורבות חלקית מאוד ולא מספקת של דירקטוריוני החברות.

עוד יצוין כי רובן המוחלט של החברות אשר ביצעו הערכת סיכוני סייבר, אף קבעו תכנית לצמצום החשיפות שעלו במסגרת הערכת הסיכונים, אולם פחות משליש מהן יישמו את תכנית הצמצום במלואה.

בנוסף, מניתוח מענה החברות לשאלון עולה כי מבקרי הפנים של כ- 40% מחברות המדגם, לא ביצעו בחינה ברמה זו או אחרת של היבטי אבטחת מידע וסיכוני סייבר בארגון במסגרת ביקורות הפנים שבוצעו על ידם בשלוש השנים האחרונות.

עמדת סגל הרשות היא כי לצורך העלאת רמת ההתמודדות של החברות עם איומי הסייבר המשתנים בקצב מהיר בשנים האחרונות, מומלץ לבסס את מרכיבי ניהול סיכוני הסייבר שלהן בהתאם לכלים מקובלים, כגון: הערכת סיכונים באמצעות סקר סיכונים שכנגזרת ממנה תיקבע ותיושם תכנית לצמצום חשיפות אשר אותרו במסגרתה, וכן ביצוע בקרה על בחינת אופן הניהול של סיכוני סייבר באמצעות ביקורת פנים.

2. גילוי בנוגע לסיכוני סייבר ומתקפת סייבר

סעיף 39 לתוספת הראשונה לתקנות ניירות ערך (פרטי התשקיף וטיוטת תשקיף – מבנה וצורה), התשכ"ט-1969 מסדיר, בין היתר, את חובות הגילוי ביחס לגורמי הסיכון של התאגיד. באוקטובר 2018 הבהירה מחלקת תאגידיים ברשות ני"ע באמצעות העמדה המשפטית, כי סיכון סייבר מהווה את אחד מגורמי הסיכון האפשריים שעשויים לחול על תאגידיים מדווחים, ולפיכך ככל שקיים בתאגיד סיכון סייבר מהותי הרלוונטי לפעילותו³, חלה חובת גילוי באשר לגורם סיכון זה, כאשר על הגילוי לכלול תיאור של הסיכון, התייחסות לקיומה של מדיניות הגנה, פיקוח על יישומה ובדיקת האפקטיביות שלה וכן את דירוג השפעתו של הסיכון על החברה (בסולם השפעה נמוך/ בינוני/ גבוה).

מתן גילוי בנוגע להיבטי סייבר עשוי להידרש מתאגיד מדווח בתשקיף ובדוח תקופתי, בדוח הדירקטוריון וכן במסגרת דיווחים מיידיים.

לעניין אופן דירוג הסיכון יצוין, כי המטרה היא שהגילוי יתייחס לסיכון השיורי לו חשופה החברה הלכה למעשה, ולא לסיכון השורשי. נזכיר כי סיכון שורשי הוא הסיכון המובנה מעצם הפעילות שמקיימת חברה, בהתעלם מהבקורות הקיימות והמאפיינים הייחודיים לתהליך, ואילו סיכון שיורי הוא הסיכון לו חשופה החברה בפועל, בהתחשב בבקורות הקיימות ובמאפיינים הייחודיים לתהליך בחברה.

מתודולוגיית דירוג סיכון הסייבר ואופן יישומה

לצורך מתן גילוי איכותי ביחס לגורמי הסיכון של החברה, ובפרט סיכון הסייבר, נבחן במסגרת הביקורת אופן קביעת דירוגו של סיכון זה על ידי חברות המדגם במסגרת דוחותיהן, היינו מהי מתודולוגיית הדירוג שאומצה על ידן וכיצד מיושמת הלכה למעשה. מתוצאות ניתוח מענה החברות לשאלון עולה, כי רק כ- 18% מהחברות מתבססות על מתודולוגיה סדורה להערכת סיכונים דוגמת סקר סיכונים, בבואן לשקול דיווח על סיכון סייבר כגורם סיכון בחברה, כ- 42% מהחברות מבצעות הערכת סיכונים בהתבסס על ידע וניסיון של ההנהלה בלבד, ולכ- 40% מהחברות הנותרות אין מתודולוגיה סדורה בעניין זה כלל.

³ יצוין כי במסגרת העמדה המשפטית פורטו גורמים אותם רצוי שיבחן תאגיד במסגרת בחינת מהותיות סיכוני הסייבר.

עוד נציין כי בחלק מחברות המדגם נמצא כי הדירוג בדוחות התקופתיים התייחס לסיכון השורשי, חלף דירוג הסיכון בהתאם לסיכון השירי לו חשופה החברה בפועל.

עמדת סגל הרשות היא כי על מנת להבטיח את גילוי כלל גורמי הסיכון הרלוונטיים לחברה במסגרת דוחותיה התקופתיים, לרבות סיכוני סייבר ואבטחת מידע, מומלץ על יישום תהליך הערכת סיכונים סדור המתבסס על מתודולוגיה מקובלת דוגמת סקר סיכונים, אשר יהווה בסיס לדיון בדירקטוריון החברה בנוגע לגורמי הסיכון לחברה, דירוגם וגילויים במסגרת הדוחות התקופתיים, כנדרש על פי דין. יצוין כי באופן כללי, יש לקחת בחשבון בבחינת מהותיות הסיכון את ההסתברות לקרות האירוע וההשפעה האפשרית שלו (עוצמת הנזק).

עוד יודגש כי על התאגידים להקפיד כי דירוג השפעת הסיכון על החברה יתבצע בהתייחס לסיכון השירי לו חשופה החברה הלכה למעשה, שהוא כאמור הסיכון לו חשופה החברה בפועל, בהתחשב בבקורות הקיימות ובמאפיינים הייחודיים לתהליך בחברה.

3. היערכות מוקדמת להתמודדות עם תקיפות סייבר

בשנים האחרונות, נאלצות חברות רבות במשק, ביניהן לא מעט תאגידים מדווחים, להתמודד עם מספר לא מבוטל של תקיפות סייבר. תקיפת סייבר, שמוגדרת כתקיפה במרחב הסייבר אשר מסכנת נכסי סייבר או מערכות ותשתיות הנתמכות על ידם, נחשבת לאירוע חירום מיוחד הדורש היערכות מקדימה, כפי שצוין גם במספר סעיפים לעיל.

3.1 נוהל גילוי על התרחשות מתקפת סייבר מהותית

תקנה 36(א) לתקנות דוחות תקופתיים ומיידיים, התש"ל-1970, שעניינה "אירוע או ענין החורגים מעסקי התאגיד הרגילים", מסדירה את חובותיו של התאגיד המדווח בנוגע לדיווחים מיידיים בקרות אירוע החורג מעסקי התאגיד הרגילים או אירוע שיש בו כדי להשפיע באופן משמעותי על מחיר ניירות הערך של התאגיד, כאשר למעשה המחוקק מכוון לאירועים אשר הם מהותיים לציבור המשקיעים בבואם לקבל החלטות השקעה. תקיפת סייבר עשויה להיחשב אירוע מהותי בהתאם להשפעתה על פעילות התאגיד או על מחיר ניירות הערך שלו. עקב כך, בקרות תקיפת סייבר, תאגיד נדרש, בין היתר, לשקלל את פוטנציאל הנזק ואת מכלול הנזק שנגרם לו או שעתיד להיגרם לו, הן במישרין והן בעקיפין, ולבחון את הצורך בדיווח לציבור לאור מהותיות האירוע. היערכות מוקדמת של תאגיד להתמודדות עם תקיפת סייבר, למשל באמצעות עיגון נהלים ותהליכים הקשורים לחובות הגילוי של התאגיד, עשויה להקל על התנהלותו בעת משבר.

מניתוח מענה החברות לשאלון עולה כי אצל כ- 76% מחברות המדגם לא קיימת התייחסות כלל לתקיפות סייבר במסגרת נוהל רלוונטי, כאשר כ- 58% מחברות המדגם כלל לא הסדירו את תהליך הגילוי הנוגע לאירוע מהותי כלשהו במסגרת נהלי עבודה.

כאמור, היערכות מוקדמת להתמודדות עם תקיפת סייבר, עשויה להקל על התנהלות תאגיד בעת משבר. עמדת סגל הרשות היא כי רצוי שהיערכות זו תכלול גם קביעת נהלים ותהליכים הקשורים לחובות הדיווח של החברה, ובין היתר, עיגון תהליכים ונהלים

נדרשים לעניין גילוי בעת קרות תקיפת סייבר מהותית. כן מומלץ להתייחס לצורך בקיומו של דיון בדירקטוריון החברה לצורך קביעת מהותיות האירוע ובחינת הצורך במתן גילוי בעניינו, כאשר באופן כללי, מהותיות נדרשת להיבחן בהתאם לפרמטרים כמותיים ואיכותיים (לעניין זה ראו גם סעיף 4 להלן).

3.2 צוות תגובה

מרכיב חשוב בהיערכות מוקדמת להתמודדות עם תקיפת סייבר הוא הקמת צוות תגובה מיומן, המיועד לתת מענה ראשוני בעת קרות האירוע.

מניתוח המענה לשאלון עולה, כי כמעט מחצית מחברות המדגם לא מינו צוות תגובה לצורך מתן מענה במקרה של תקיפת סייבר. כמו כן, מניתוח מענה החברות לשאלון עולה כי כמחצית מהחברות אשר כן מינו צוות תגובה למתקפת סייבר, אינן מקיימות תרגולים או הדרכות באופן עיתי עבור צוות זה.

כפי שצוין לעיל, להיערכות מקדימה יש חשיבות רבה ליכולת חברה להתמודד ביעילות עם אירוע סייבר. מומלץ כי במסגרת ניהול אפקטיבי של סיכוני סייבר, תובא בחשבון גם בחינה של נחיצות מינוי צוות תגובה, לרבות אופיו, הרכבו, סמכויותיו והכשרתו.

4. מתקפות סייבר וגילוי על התרחשותן

מתקפות סייבר שאיתן מתמודדים תאגידיים, מטופלות לרוב על ידי פונקציות העוסקות בפן הטכנולוגי בארגון. כאמור לעיל, קיימת חשיבות רבה כי גם הצד העסקי יהיה מעורב בטיפול, או לכל הפחות יהיה מעודכן בפרטי התקיפה תוך בחינת השפעתה על תהליכיו העסקיים של התאגיד. מעורבות הצד העסקי וקיום תקשורת תקינה בין אנשי הטכנולוגיה להנהלת התאגיד נדרשים גם לצורך קביעת מהותיות האירוע ובחינת הצורך במתן גילוי פומבי לגביו.

מניתוח מענה החברות לשאלון עולה, כי כרבע מחברות המדגם חוו לפחות תקיפת סייבר אחת ברמה כלשהי בשלוש השנים האחרונות, כאשר רובן חוו תקיפה אחת בלבד בתקופה זו. עוד עולה, כי כ-40% מהחברות שחוו לפחות מתקפת סייבר אחת בשלוש השנים האחרונות, לא קיימו דיון בדירקטוריון או בהנהלה ביחס למהותיות האירוע ולצורך במתן גילוי פומבי לגביו, ו-17% נוספים מהחברות קיימו דיון בדירקטוריון רק ביחס לחלק מן התקיפות שחוו.

כאמור לעיל, היערכות מקדימה מצד החברות, הכוללת, בין היתר, הסדרה מראש של נהלים ותהליכי עבודה שיטתיים רלוונטיים, תאפשר לחברות לנהל ולהתמודד בצורה אפקטיבית יותר עם תקיפת סייבר בפועל. עמדת סגל הרשות היא כי במסגרת הקווים המנחים שייקבעו לעניין זה בנהלי עבודה, מומלץ להתייחס לצורך בקיומו של דיון בדירקטוריון החברה או בהנהלתה הבכירה לצורך קביעת מהותיות האירוע ובחינת הצורך במתן גילוי בעניינו (לעניין זה ראו גם סעיף 3.1 לעיל).