אם אינך רואה מייל זה לחץ כאן

עמדה משפטית מס' 105-33 של סגל רשות ניירות ערך: גילוי בנושא סייבר

11/11/2018

ביום 21.10.18 פרסמה רשות ניירות ערך (להלן: "**הרשות**") עמדת סגל מס' 105-33 בדבר גילוי בנושא סייבר (להלן: "**עמדת הסגל**"), שמטרתה הגברת מודעות התאגידים המדווחים לסיכוני סייבר ומתן דגש להיבטים מסוימים אשר הגילוי לגביהם עשוי להידרש על פי דיני ניירות הערך. עמדת הסגל עוסקת בדיווח הן אודות "תקיפת סייבר", אשר הוגדרה כפעילות שנועדה לפגוע בשימוש במחשב או בחומר מחשב השמור בו, והן אודות "סיכון סייבר" שהוגדר כסיכון להתרחשות תקיפת סייבר.

עמדת הסגל פורסמה על רקע עליית נושא ההתמודדות מול איומי הסייבר לסדר היום הציבורי והתאגידי. בשנים האחרונות תקיפות הסייבר הפכו למתוחכמות והרסניות יותר. קצב השינויים המהיר בעולם הטכנולוגי, החדשנות וזמינות המידע יוצרים מחד הזדמנויות עסקיות מגוונות, ומנגד תלות בכלים מחשוביים. סביבה זו מייצרת חשיפות ואיומים חדשים, שלעיתים קשים לזיהוי ודורשים מומחיות באיתורם, מניעתם, בהתאוששות מפגיעתם ובמזעור נזקים. איומי סייבר עשויים לנבוע מסוגים שונים של תקיפות ומגורמים שונים של מתקיפים, פנים ארגוניים וחוץ ארגוניים, הפועלים כלפי התאגיד עצמו או גורמים הקשורים אליו. היקף החשיפות לסיכוני סייבר משתנה מתאגיד לתאגיד ותלוי בגורמים רבים ומגוונים. תקיפת סייבר עלולה לגרום לנזקים ישירים ועקיפים, ובמקרים מסוימים עלולים הנזקים הכלכליים והעסקיים להגיע להיקף משמעותי עד כדי פגיעה מהותית בתפקוד התאגיד ובהמשכיות העסקית שלו. השפעת איומי הסייבר כסיכון משתנה תדיר עלולה להיות מהותית לתאגיד גם אם לא התממשו האיומים, וזאת למשל כתוצאה מעלויות הכרוכות בשיפור או חיזוק מערך הגנת הסייבר. ייתכנו גם עלויות עקיפות נוספות, כגון עלויות הנובעות מהאטת תהליכים בתאגיד כתוצאה משינוי נהלי האבטחה הפנים ארגוניים.

עמדת הסגל מבהירה כי אין בה כדי ליצור חובות גילוי חדשות. עניינה הוא, אפוא, בהפניית תשומת הלב לתחולת העקרונות הכלליים של דיני ניירות ערך בסביבה הטכנולוגית המשתנה, ובהקשר הספציפי של סיכוני הסייבר. לכן, גילוי בענייני הסייבר יהיה כפוף, ככל גילוי אחר, למבחני המהותיות הרלוונטיים. כך, לא יידרש תיאור גנרי של סיכוני סייבר כלליים שכלל התאגידים המדווחים חשופים אליהם, ולא יידרש גילוי טכני מפורט שלהם, שאינו בעל ערך למשקיע הסביר בניירות הערך של התאגיד.

עמדת הסגל מפנה לדרישות הגילוי הקיימות בדין בקשר לגורמי סיכון או התממשותם,

ובהן הדרישות העיקריות המפורטות להלן.

1. <u>גילוי בתשקיף ובדוח התקופתי</u>

1.1. גורמי סיכון

סעיף 39 בתוספת הראשונה לתקנות ניירות ערך (פרטי התשקיף וטיוטת התשקיף – מבנה וצורה), התשכ"ט – 1969 (להלן: "**התוספת הראשונה**") מסדיר את חובות הגילוי ביחס לגורמי הסיכון של התאגיד. סיכון סייבר הינו גורם סיכון ככל סיכון אחר. במידה וקיים בתאגיד סיכון סייבר מהותי הרלוונטי לפעילותו, על הגילוי בדבר סיכון זה לכלול את תיאור הסיכון, התייחסות לקיומה של מדיניות הגנת סייבר, פיקוח על יישומה ובדיקת האפקטיביות שלה. לעניין זה, הגנת סייבר כוללת את מדיניות התאגיד בדבר מכלול הפעולות הנדרשות למניעה, להתמודדות ולטיפול בתקיפת סייבר או סיכון סייבר, לצמצום השפעתם והנזק הנגרם מהם, במהלכם ואחריהם, ובכלל זה, פעולות אבטחת מידע. עמדת הסגל מונה גורמים שונים אשר עשויים לסייע בבחינת מהותיות סיכוני הסייבר, כגון תקיפות קודמות, ההסתברות להתרחשותן, יכולות התאגיד להתמודד עמן, המשאבים הכרוכים בהגנת סייבר ופוטנציאל הפגיעה בנכסים.

1.2. גילוי על אירועים החורגים מעסקי התאגידים הרגילים

סעיף 36 בתוספת הראשונה מסדיר את חובות הגילוי במקרה של אירוע או עניין החורגים מעסקי התאגיד הרגילים בשל טיבם, היקפם או תוצאתם האפשרית, ואשר יש להם או עשויה להיות להם השפעה מהותית על התאגיד. לכן, אם התרחשה בתקופת הדוח תקיפת סייבר מהותית, על התאגיד לבחון את הצורך בהכללה של תיאור תמציתי שלה בדוח התקופתי. גילוי כאמור יכלול התייחסות לפרטים רלוונטיים, ובהם נסיבות התקיפה, היקף וסוג הנזק שנגרם לרבות השלכות עקיפות, הפקת לקחים ופעולות הגנת סייבר שננקטו על ידי התאגיד כדי למנוע תקיפה חוזרת.

2. <u>גילוי בדוח הדירקטוריון</u>

במקרה בו התאגיד סבור שחשיפתו לסיכוני סייבר הפכה בשנת הדוח למהותית יותר להבנת פעילותו באופן כללי, או במקרה בו אירעו בתקופת הדוח תקיפות סייבר בעלות השפעה מהותית על עסקי התאגיד, יכלול דוח הדירקטוריון על מצב עסקי התאגיד את הסברי הדירקטוריון בנושא (תקנות 10 ו-6 בתקנות ניירות ערך (דוחות תקופתיים ומיידיים), התש"ל-1970 (להלן: "**תקנות הדוחות**"). הסברי הדירקטוריון יתייחסו להשפעת חשיפות ואירועים כאמור על הסעיפים הספציפיים בדוחות הכספיים, כגון לקוחות, מלאי ונכסים לא מוחשיים (סעיפים מאזניים) או אובדן הכנסות, ירידת ערך, הפרשות ופגיעה ברווחיות (סעיפים תוצאתיים). בנסיבות המתאימות, התיאור יתייחס גם להשלכות תקיפת סייבר אשר טרם קיבלו ביטוי בדוחות הכספיים, כגון במקרה של הגשת תביעות, פגיעה בפעילות התאגיד, במוניטין שלו, או בתיק הלקוחות שלו.

3. <u>גילוי בדוחות מיידים</u>

בהתאם לתקנה 36(א) בתקנות הדוחות, תאגיד נדרש לדווח על אירוע או עניין החורגים מעסקי התאגיד הרגילים בשל טיבם, היקפם או תוצאתם האפשרית, ואשר יש להם או עשויה להיות להם השפעה מהותית על התאגיד או שיש בהם כדי להשפיע באופן משמעותי על מחיר ניירות הערך שלו. בהתאם, במקרה בו מתרחשת תקיפה סייבר, התאגיד נדרש לבחון את מהותיות האירוע, ולשם כך עליו לשקלל את גובה הנזק ופוטנציאל הנזק (במישרין ובעקיפין). אירועים אשר עשויים להיות ברי-דיווח כוללים, לדוגמה, מקרים של הפסקת הפעילות העסקית של התאגיד, גרם נזק למערכות מיחשוב מהותיות, פריצה למאגרי מידע של התאגיד או חשיפת סודות עסקיים שלו, וגילוי פירצות אבטחה.

על התאגיד לכלול במסגרת הדיווח המיידי כל פרט חשוב להערכת השלכות האירוע, ובכלל זה, תיאור האירוע, ותיאור והערכת הנזק שלו, לרבות ההשפעה האפשרית על תוצאות הפעילות ועל המוניטין שלו. כמו כן, יכול שיידרשו דיווחים משלימים על האירוע על פי תקנה 37א2 בתקנות הדוחות, ככל שיחולו התפתחויות מהותיות מאוחרות למועד הדיווח המיידי המקורי.

<u>מידע נוסף</u>

לעמדת סגל רשות ניירות ערך מספר 33-105: גילוי בנושא סייבר, לחץ <u>כאן</u>.

פרטי קשר:

ד"ר שאול חיון, שותף
מחלקת שוק ההון

shaulh@meitar.com | 03-6103723

למידע נוסף אודות מחלקת שוק ההון במשרדנו, לחץ כאן.