

## G-CAPITAL - חובות הגילוי לתאגיד בעקבות איומי הסייבר

23 באוקטובר, 2018

ביום 21.10.18 פרסמה רשות ניירות ערך עמדת סגל משפטית בדבר "גילוי בנושא סייבר". כמוכנה בעמדה, מטרתה היא להגביר את מודעות התאגידים המדווחים לסיכוני הסייבר ולתת דגש להיבטים מסוימים אשר הגילוי לגביהם עשוי להידרש על פי הוראות דיני ניירות ערך. עמדת הסגל מפרטת את דרישות הגילוי השונות אשר קיימות בדין באשר לסיכוני הסייבר ולמקרים של התממשותם. להלן נעמוד על עיקרי העמדה.

### • גילוי בתשקיף ובדו"ח התקופתי

**דיון בגורמי סיכון** - לעניין חובות הגילוי ביחס לגורמי הסיכון של התאגיד<sup>1</sup>, סגל הרשות הבהיר כי סיכוני סייבר הנם "גורם סיכון" ככל סיכון אחר. אם קיים בתאגיד סיכון סייבר מהותי הרלוונטי לפעילותו, יש לכלול גילוי בתשקיף בדבר סיכון זה, לרבות תיאור הסיכון, התייחסות לקיומה של מדיניות הגנה, פיקוח על יישומה ובדיקת האפקטיביות שלה.

בעמדה פורטה רשימה של גורמים שרצוי בין היתר לשקול בעת בחינת מהותיות סיכוני הסייבר, לרבות התרחשותן של תקיפות סייבר קודמות, חומרתן ותדירותן; ההסתברות להתרחשות תקיפות סייבר; אפקטיביות ההגנה של התאגיד; סיכונים ספציפיים לפעילות התאגיד; המשאבים הכרוכים בשמירה על הגנות סייבר לרבות הכיסוי הביטוחי המתייחס לתקיפות סייבר; ושיקולים נוספים הרלוונטיים לתאגיד.

**גילוי על אירועים החורגים מעסקי התאגיד הרגילים** - לעניין חובת הגילוי במקרה של אירוע או ענין החורגים מעסקי התאגיד הרגילים<sup>2</sup>, סגל הרשות הבהיר כי במקרה של תקיפות סייבר מהותיות שהתרחשו בתקופת הדוח, על התאגיד לבחון תיאור תמציתי של עיקרי האירועים שהתרחשו או הכללה על דרך ההפניה לדוחות מידיים שפרסם התאגיד שבמסגרתם תוארו האירועים כאמור.

התיאור יכלול את הפרטים הרלוונטיים בדבר התקיפה, למיטב ידיעת התאגיד, כגון זהות או סוג התוקפים, כמות התקיפות ומשך זמן התקיפה, האם להערכת התאגיד התקיפה הסתיימה, נזקים והשלכות ישירות ועקיפות, האמצעים שנקטו, פעולות מנע והפקת לקחים. גם במקרה של מספר

<sup>1</sup> בהתאם לסעיף 39 לתוספת הראשונה לתקנות ניירות ערך (פרטי התשקיף וטיוטת התשקיף - מבנה וצורה), התשכ"ט-1969 ("התוספת הראשונה לתקנות פרטי תשקיף").

<sup>2</sup> בהתאם לסעיף 36 לתוספת הראשונה לתקנות פרטי תשקיף.

אירועים שאינם מהותיים אשר במקובץ מגיעים לכדי השפעה מהותית, נדרש התאגיד לבחון גילוי כאמור.

#### • גילוי בדו"ח הדירקטוריון

סגל הרשות הבהיר, כי ככל שסבור תאגיד שחשיפתו לסיכוני סייבר הפכה בשנת הדוח למהותית יותר להבנת פעילותו באופן כללי, או אם אירעו תקיפה או תקיפות סייבר בעלי השפעה מהותית על אחד או יותר מסעיפי הדוחות הכספיים (מאזני או תוצאתי), יובאו הסברי הדירקטוריון בעניין זה בדו"ח הדירקטוריון.

עוד הובהר כי הסברי הדירקטוריון ייתכן שיידרשו אף אם אין לאירוע השפעה ישירה על הדוחות הכספיים אך פרטי האירוע תוארו כחלק מתיאור עסקי התאגיד במסגרת הדוח התקופתי. במסגרת ההסברים תינתן התייחסות להשפעת האירועים על סעיפים מהדוחות הכספיים שהושפעו מהותית בשל סיכוני סייבר או תקיפות סייבר, כגון השפעות על סעיפים מאזניים (כגון לקוחות, מלאי, רכוש בלתי מוחשי), השפעות על סעיפים תוצאתיים (כגון אובדן הכנסות, הפרשות), סך עלויות הנובעות מהגנת סייבר, והשפעת תקיפות סייבר אשר טרם קיבלו או לא יקבלו ביטוי במסגרת הדוחות הכספיים אך הם מהותיים לפעילות התאגיד (כגון, פגיעה בפיתוח מוצר, פגיעה בתיק לקוחות, פגיעה במוניטין).

#### • גילוי בדיווחים מידיים

סגל הרשות הבהיר כי בקורות תקיפת סייבר תאגיד נדרש לבחון את מהותיות האירוע לצורך דיווח, ולשם כך לשקלל את מכלול הנזק ופוטנציאל הנזק שגרמה תקיפת הסייבר, הן במישרין והן בעקיפין.

סגל הרשות ציין מספר דוגמאות לאירועים אשר לעמדתו עשויים לחייב בדיווח מידי, כגון: הפסקת פעילותו העסקית של התאגיד לפרק זמן; פריצה למאגרי המידע של התאגיד באופן שעלול להשפיע על פעילות התאגיד במישרין או בעקיפין; נזק למערכת מחשוב המהותית לפעילות התאגיד; דרישת תשלום כופר בסכום מהותי; חשיפת "ציתות" למערכות המחשוב של התאגיד על ידי גורמים עוינים; גילוי של גניבת מידע עסקי פרטי שחשיפתו עלולה לפגוע מהותית בתאגיד או גילוי פרצת אבטחת סייבר במוצרי החברה או במערכות שהחברה בנתה או אחראית להן שבגינה קיימת חשיפה לחברה כיצרנית או ספקית המוצר וכדומה.

הדיווח המידי יכלול כל פרט חשוב להערכת האירוע המדווח על עסקי התאגיד, ובכלל זה תיאור האירוע (מועד תחילת האירוע ומועד סיומו, מה כלל האירוע, סוג הנתונים שנחשפו והצעדים שנקט התאגיד בעניין), תיאור הנזק והערכת הנזק, לרבות פגיעה אפשרית בהכנסות ומידת הפגיעה ביחסי לקוחות, ספקים ומוניטין של התאגיד. עד כמה שניתן, יש להתייחס להערכה כוללת של הנזק הצפוי. סגל הרשות הבהיר שיתכן גם צורך בדיווחים משלימים, בהתאם לתקנה 37(ה)2 לתקנות הדוחות, למשל בעקבות פגיעה נמשכת בנכסים, עלויות מהותיות להקמת מערכות הגנה חדשות וכדומה.

סגל הרשות הבהיר שאין בעמדה כדי ליצור חובות גילוי חדשות וכל גילוי בהתאם לעמדה כפוף למבחני המהותיות הרלוונטיים לפי הדין. כך למשל, לעמדת סגל הרשות, תאגיד אינו נדרש לתאר סיכוני סייבר כלליים וזאת על מנת למנוע דיווחים גנריים שמהותיות האמור בהם למשקיע שולית או לא קיימת. כמו כן, סגל הרשות הבהיר כי התאגיד אינו נדרש למסור גילוי טכני ומפורט באופיו בענייני סייבר, אלא לנהוג בהקשר זה על פי דרישות ופרקטיקות הגילוי המקובלות גם בנושאים אחרים. יש לציין כי אין בעמדה כדי להוות רשימה ממצה של כל חובות הדיווח החלות על תאגיד בקשר עם איומי סייבר.

משרדנו עומד לרשותכם בכל שאלה או הבהרה בקשר עם חובות הגילוי החלות על התאגיד על רקע איומי סייבר או תקיפות סייבר, כמו גם בקשר עם היערכות מראש להתמודדות עם החשיפות בתחום זה. למידע נוסף:

[sagy@gornitzky.com](mailto:sagy@gornitzky.com)

[shiloni@gornitzky.com](mailto:shiloni@gornitzky.com)

[assafh@gornitzky.com](mailto:assafh@gornitzky.com)

עו"ד שרון ורקר-שגיא, שותפה

עו"ד יאיר שילוני, שותף

עו"ד אסף הראל, שותף

לעמדת סגל הרשות: [לחץ כאן](#)

המידע הכלול במסמך זה הינו מידע כללי ותמציתי בלבד, אינו מחליף את הצורך בעיון מלא ומעמיק בנוסח המלא של ההחלטה/הפרסום/הוראת החוק הרלוונטיים, הוא אינו מהווה חוות דעת משפטית או יעוץ משפטי ואין להסתמך עליו.

להרשמה לרשימת התפוצה נא לפנות למערכת G-Capital Market בכתובות המייל הרשומות לעיל.