

ביטוח סיכוני סייבר

בשנת 2018 ה- **World Economic Forum** הגדיר את סיכון הסייבר כאחד מחמשת הסיכונים המשפיעים ביותר על ממשלות, ארגונים וחברות בעולם. הנזק לתאגיד כתוצאה מאירוע סייבר מתבטא בתביעות כספיות, אבדן לקוחות, אבדן הכנסה, נזק למוניטין, אבדן המשכיות עסקית, והוצאות כספיות משמעותיות (כגון: תשלומי כופר, הוצאות הודעה ללקוחות, הוצאות פורנויות לצורך גילוי הפריצה, הוצאות לניהול המשבר בתקשורת, פיצויים מוסכמים וכן קנסות רגולטוריים).

כיום, **מרבית התאגידים חשופים לסיכוני סייבר**, אולם רמת המוכנות וההגנה אינה נותנת מענה מלא לחשיפות עמן הם מתמודדים. בנוסף, טיפול רשלני בסיכוני הסייבר עלול לגרור אחריות אישית של נושאי המשרה בתאגיד.

ביטוח סייבר מסייע בהקטנת החשיפות הפיננסיות כתוצאה מאירוע סייבר.

רכישת ביטוח סייבר הינה מורכבת, ודורשת ייעוץ מקצועי בנוגע להיבטים רגולטוריים, היבטים משפטיים, חשיפות כלפי צדדים שלישיים, אבטחת מידע ועוד. קיימת חשיבות רבה לליווי מקצועי הן בשלב המקדמי של מילוי השאלונים המשמשים בסיס חיתומי עבור חברות הביטוח, והן בעת ניהול המשא ומתן לגבי היקף הפוליסה והתאמתה לצרכים הייחודיים של התאגיד.

בסקירה זו נדון במספר מגמות עכשוויות, המרחיבות משמעותית את החשיפה של החברה ושל נושאי המשרה בה לסיכוני סייבר והשלכותיהם. בנוסף, נעמוד על עיקרי הכיסוי בביטוח סייבר ונסקור את השינויים ברגולציה הישראלית בתחום זה.

מגמות עכשוויות המרחיבות את סיכון הסייבר לחברה ולנושאי המשרה:

1. עובדי החברה:

עובדי החברה הם אחד הגורמים המשמעותיים ביותר לנזקי אבטחת מידע בארגונים, הן כתוצאה ממעשה רשלני (שימוש רשלני בהרשאות גישה או מעשה או מחדל בתום לב) והן כתוצאה ממעשה מכוון.

2. שינויים רגולטורים בתחום הגנת המידע:

העלייה המשמעותית שאנו חווים לאחרונה ברמת הרגולציה ואכיפתה בתחום הגנת הפרטיות מייצרת חשיפה מוגברת. תקנות הגנת הפרטיות בישראל, כמו רגולציית ה-GDPR באירופה ומקבילותיה במדינות השונות, מטילות אחריות מוגברת על חברות ועל נושאי משרה במדינות רבות בתחום הגנת המידע. חבות אישית של נושאי משרה, בנוסף לקנסות רגולטוריים משמעותיים ביותר על החברה, עלולים לגרום לנזק משמעותי לחברה (לדוגמה, קנס מכוח חקיקת ה-GDPR עלול להגיע עד ל-20 מיליון אירו או 4% מהכנסות החברה בכל העולם, הגבוה מביניהם).

3. **חשיפה לחברי הדירקטוריון ונושאי המשרה:**

ניהול סיכוני סייבר הפך לאחד מנושאי הליבה באחריות הדירקטוריון. לאחרונה, אנו עדים לגידול במספר התביעות הייצוגיות בעולם הנובעות מכשל באבטחת המידע ו/או הפרת פרטיות. רגולטורים שונים, דוגמת ה-SEC בארה"ב והרשות לניירות ערך בישראל, דורשים גילוי בדוחות הכספיים של חברות ציבוריות לגבי סיכוני ואירועי הסייבר. בהקשר זה רצוי לוודא כי פוליסת נושאי המשרה אשר ברשות החברה מכילה כיסוי מתאים לתביעה בגין נזק סייבר.

4. **מיזוגים ורכישות (M&A):**

הטמעת מערכות מידע של חברה נרכשת הינה בעלת פוטנציאל סיכון סייבר משמעותי לחברה הרוכשת. ברוב המקרים, לא ניתן במסגרת בדיקות הנאותות המוגבלות בזמן קצוב, לאתר את כל נקודות התורפה של אבטחת המידע בחברה הנרכשת. בנוסף, יש להטמיע נהלי אבטחת מידע ולייצר מודעות בקרב העובדים החדשים.

5. **חשיפה הנובעת מספקים / צדדים שלישיים:**

ההסתמכות ההולכת וגדלה של חברות על ספקי שירות (צדדים שלישיים) בייצור ההכנסה של החברה, מגבירה משמעותית את החשיפה לסיכוני סייבר. דוגמה נפוצה היא העברת ה-Data Center של חברות לשירותי Cloud אשר הינם בבעלות צד שלישי ואשר לחברה אין יכולת לשלוט על רמת אבטחת המידע בהם.

6. **שימוש בטכנולוגיה לצורך יעילות תפעולית:**

חברות רבות משתמשות בטכנולוגיות שונות על מנת לייצר יעילות תפעולית. מערכות בקרה ושליטה טכנולוגיות לצורך ניהול תהליכי הייצור הינן דוגמה נפוצה לכך. חדירה למערכות הבקרה והשליטה של מפעל לייצור דלק לדוגמה, יכולה לגרום לנזקי גוף ורכוש משמעותיים ביותר. דוגמה נוספת היא השימוש ההולך וגובר של עיריות בשרותי "Smart City", אשר חושף מערכות כמו מערכת הרמזורים או נתונים פרטיים של אזרחים לפריצות סייבר.

7. **האינטרנט של הדברים (IoT):**

מכשירי IoT נמצאים כבר היום בחברות רבות ומספרם צפוי לגדול משמעותית עם המעבר לטכנולוגיית 5G. לדוגמה, מערכות לשיחות ועידה, מצלמות אבטחה, מדפסות, מערכות חיישנים ואוטומציה, מחוברות לרשת ולמערכות ה-IT של החברה. פריצה למערכות המידע של החברה באמצעות חדירה למכשירי IoT עלולה להגדיל משמעותית את החשיפות.

ניהול סיכון הסייבר כולל שני שלבים עיקריים:

1. **זיהוי ומיפוי הסיכונים והנכסים המהותיים לתאגיד:** מידע פרטי של לקוחות, מידע פרטי של עובדים, קניין רוחני, ומידע עסקי כגון רשימת לקוחות, תכניות עסקיות, תכניות אסטרטגיה, מוניטין ועוד.

2. **יצירת תשתית אירגונית להתמודדות עם סיכוני הסייבר הכוללת ניהול, יישום, אכיפה ובקרה של תכניות ונהלים** פנים ארגוניים להפחתת הסיכון. ביטוח סייבר מהווה חלק מהתשתית הארגונית לטיפול בסיכון ומעטפת הגנה נוספת מפני נזקי סייבר.

כיסוי בגין נזק כספי לתאגיד:

- אבדן הכנסה.
- הוצאות דמי כופר.
- הוצאות דיווח ללקוחות.
- הוצאות פורנזיות לגילוי הכשל באבטחת המידע.
- הוצאות בגין משרד יחסי ציבור לניהול המשבר.
- הוצאות חקירה רגולטורית.
- קנסות רגולטוריים.

כיסוי בגין נזק לצד שלישי:

- תביעה בגין הפרת פרטיות של צד שלישי.
- תביעה בגין כשל באבטחת מידע של צד שלישי.
- תביעה בגין קנסות רגולטוריים לצד שלישי.
- הוצאות חקירה רגולטורית.
- הוצאות משפטיות.

נתונים המשפיעים על היקף הכיסוי בפוליסה:

היקף ותנאי פוליסת הסייבר נקבעים על ידי המבטחים בכפוף לתהליך חיתומי הכולל בין היתר שאלון מפורט לגבי היקף וטיב המידע המצוי בבעלות ו/או המוחזק על ידי התאגיד, תחומי הפעילות העסקית של התאגיד, רמת והיקף אבטחת המידע בחברה, אירועי ונזקי סייבר קודמים ופרמטרים נוספים.

חברות הביטוח מתנות כיסוי זה בבדיקות מקיפות אשר עשויות לצמצם את תכולת הכיסוי ואף להתבטא בעלויות משמעותיות.

על מנת שהכיסוי הנרכש ייתן מענה מיטבי וכלכלי לחשיפות הייחודיות של כל חברה, נדרש ליווי מקצועי בעת הליך רכישת הפוליסה.

רגולציה ישראלית בתחום הגנת הפרטיות

תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז – 2017, אשר נכנסו לתוקף במאי 2018, מטילות חובות משמעותיות על הבעלים, המנהלים והמחזיקים של מאגרי מידע בישראל לאבטחת המידע שברשותם. התקנות עוצבו במתכונת מודולארית, המכילה חובות ברמה הולכת וגדלה לפי רמת הסיכון שיוצרת פעילות עיבוד המידע בארגון, בהתחשב בגודל המאגר, ברגישות המידע ובמספר המורשים לגשת אליו. בעלי מאגרי המידע מחויבים:

- להגדיר במסמך הגדרות המאגר את מטרות המאגר, את סוגי השימושים בו, את הסיכונים העיקריים לפגיעה באבטחתו ואת דרכי ההתמודדות עמם.
- למנות ממונה על אבטחת המידע.
- לקבוע נוהל לאבטחת מידע הכולל אבטחה פיזית, ניהול הרשאות, ניהול מידע לגבי כוח אדם, ניהול הרשאות גישה, אמצעי הגנה, בקרה ותיעוד, מיפוי הסיכונים ודרכי ההתמודדות עמם.
- למפות את מערכות מאגר המידע ולבצע סקר סיכונים.

- לתעד אירועי אבטחה המעלים חשש לפגיעה במידע, שימוש ללא הרשאה או חריגה מהרשאה.
- לשמור לגבות ולשחזר נתוני אבטחה.

עמדת הרשות לניירות ערך לגבי סיכוני הסייבר (עמדה משפטית מספר 33-105): נועדה להגביר את מודעות התאגידים המדווחים לסיכון הסייבר ולתת דגש להיבטים אשר הגילוי לגביהם עשוי להידרש על פי הדצן, להלן העיקריים שבהם:

1. גילוי בתשקיף ובדו"ח התקופתי:

עמדת הרשות לניירות ערך היא כי בבוא תאגידים לבחון את גורמי הסיכון ואת תיאור עסקי התאגיד לצורך גילוי בתשקיף ובדו"ח התקופתי, כאשר קיים סיכון סייבר מהותי, יש לכלול גילוי בעניינו. כאשר בוחנים את מהותיות סיכון הסייבר יש לתת את הדעת לנושאים הבאים: התרחשויות סייבר קודמות, חומרתן ותדירותן; ההסתברות להתרחשות תקיפות סייבר; אפקטיביות יכולת התאגיד להקטין או למנוע את הסיכון; סיכוני סייבר מהותיים וההשלכות שלהם על התאגיד; המשאבים שהתאגיד מקצה לעניין זה; פוטנציאל הפגיעה בנכסים ובכללם קניין רוחני ומוניטין וכן חוקים, תקנות ורגולציה רלוונטיים. **במקרה של תקיפת סייבר מהותית** בתקופת הדוח, יש לכלול דיווח לגבי עיקרי האירועים בדוח או להפנות לדוח מיידי אשר במסגרתו ניתן דיווח כזה. עיקרי הדיווח יכללו תיאור האירוע, תיאור והערכת הנזק וכל דיווח משלים על האירוע.

2. גילוי בדו"ח הדירקטוריון:

עמדת הרשות היא כי יש לדווח בדוח הדירקטוריון על סיכוני סייבר או תקיפות סייבר אשר הינם בעלי השפעה מהותית על הדוחות הכספיים של החברה (השפעות על סעיפים מאזניים ועל סעיפים תוצאתיים).

לסיכום, סיכוני הסייבר הינם נחלת הכלל, ותאגידים נדרשים לנהל סיכונים אלו לצורך פעילותם העסקית וצמיחת התאגיד, וכן על מנת לעמוד ברגולציה המשתנה; ביטוח סייבר הינו כלי שימושי ואפקטיבי לצורך הקטנת הנזק.

עורכי הדין במשרדנו מעניקים ייעוץ מקיף בתחום ביטוח סיכוני סייבר, בדגש על איכות והיקף הכיסוי תוך התאמת פתרונות ייחודיים בהתאם לפרופיל הסיכון של כל תאגיד.

* * *

הסקירה לעיל הינה בבחינת תמצית. המידע הכלול בה נמסר למטרות אינפורמטיביות בלבד ואין במידע כדי להוות ייעוץ משפטי. לקבלת פרטים נוספים, אנא פנו לעו"ד עידו גונן, ראש תחום ביטוח וניהול סיכונים, גולדפרב זליגמן, בדוא"ל ido.gonen@goldfarb.com ו/או בטלפון 03-6089372, או לעו"ד דפנה לוטן מדוויר, שותפה, תחום ביטוח וניהול סיכונים, גולדפרב זליגמן, בדוא"ל dafna.lotan@goldfarb.com ו/או בטלפון 03-6089372