האם גופי השקעות מוסדיים צריכים להתייחס גם לסיכוני סייבר בחברות בהן הם משקיעים?!

רואי סטאל, מנכ"ל אנטרופי ניהול סיכונים ומתי אהרון, מנכ"ל אנטרופי ממשל תאגידי

אחד השינויים המרכזיים בעולם המודרני נובעים מהתפתחות הטכנולוגיה והתבססות הארגונים עליה. כיום, אסטרטגיה של כמעט כל ארגון ומכלול פעילויותיו העסקיות והתפעוליות מושתתות על שימוש בטכנולוגיה מגוונת וככל שיעבור הזמן כך תגדל התלות בטכנולוגיה, במתן שירותים דיגיטליים ללקוחות, רשתות חברתיות ועוד. ההתפתחות הטכנולוגית הינה מנוף של ארגונים להתפתחות עסקית ואסטרטגית ומתן שירותים מתקדמים נוחים, יעילים ומהירים בין אם מדובר בדיגיטציה של שירותים, שירותי ענן ועוד.

בבחינת סיכוני טכנולוגיית המידע, נדרש לקחת בחשבון התפתחות זו ולמקד את ראיית הסיכונים תוך הבנת מוקדי הסיכון החדשים שנוצרים.

תהליך הטיפול בסיכוני טכנולוגיה בארגון נמנה לגישתנו על התהליכים החשובים הנדרשים לביצוע בארגונים בעת הזו, ובתוך עולם סיכונים זה, **סיכון הסייבר הנו אחד הסיכונים המרכזיים ביותר עמו מתמודד כל ארגון**.

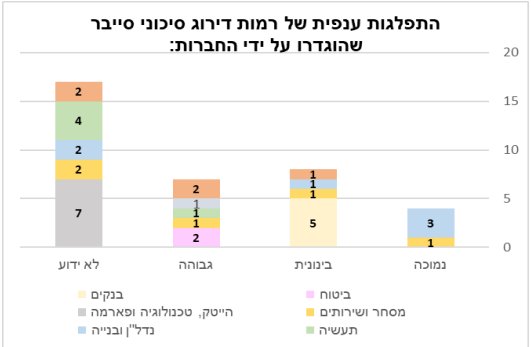
החשיפה לסיכוני סייבר קיימת כמעט בכל ארגון והולכת וגדלה בשני היבטים. האחד, לאור התלות הגוברת בטכנולוגיה אשר מגדילה את מקורות התקיפה (וקטורי תקיפה) והשני, לאור כך שההשפעה של תקיפת סייבר על ארגון הפכה למשמעותית יותר ויותר, שכן כיום מרבית עסקיו של ארגון והאסטרטגיה שלו מושתתים על טכנולוגיה וכל בסיס המידע שלו מאוחסנים באמצעים טכנולוגים.

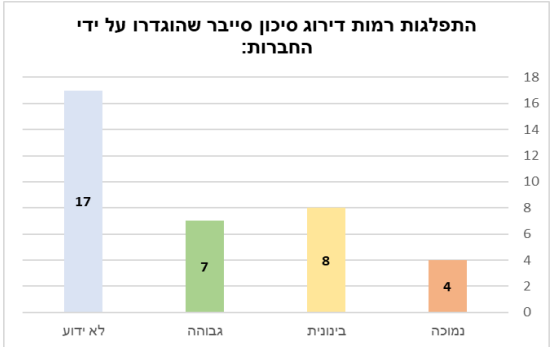
בנוסף, יש לזכור גם כי המוטיבציה של התוקפים הולכת וגדלה, שכן "יש הרבה מה להשיג" בתקיפות סייבר על ארגונים מושתתים טכנולוגיות. וקטורי התקיפה הולכים ומתרבים מידי יום, הכלים לתקיפה הופכים למתוחכמים יותר, יכולות התוקפים הולכות ומשתפרות. התוקף יכול להגיע מכל שלב בשרשרת האספקה, החל מהאקרים מבחוץ, ספקים, לקוחות וכלה בעובדי הארגון עצמו אשר מנצלים את ההכרות שלהם עם הארגון, כפי שהתרחש במספר לא מבוטל של תקיפות בעת האחרונה.

ההתמודדות של ארגונים עם סיכון הסייבר הנה יום יומית ותמידית, במיוחד במוסדות פיננסיים, גופים ביטחוניים, חברות תשתית, חברות תקשורת, חברות נסחרות ותאגידים גדולים אחרים. מידי יום ארגונים חווים עשרות ואף מאות ניסיונות תקיפה, דבר אשר אין דומה לו באף עולם סיכון אחר (רגולציה, אשראי, פיננסי וכו') ואשר בפועל הופך את סיכון הסייבר לגורם הסיכון הגדול ביותר עבור כל ארגון. נושא זה מקבל חיזוק בדוח השנתי של בנק ישראל אשר קבע כי מתקפות סייבר הן הסיכון העיקרי לבנקים.

בבחינה של החברות הציבוריות הגדולות במשק (הנמנות על מדד תא 35, *מדובר ב 36 חברות שחלקן כבר נמחק ממסחר לאחרונה) נראה כי למעלה מ 90% מהן הגדירו את נושא הסייבר כסיכון לארגון. 7 מתוכן הגדירו את הסיכון כגבוה ואילו 8 מתוכן הגידרו את הסיכון כבינוני. מעניין וחשוב לראות כי 17 מתוכן לא הגדירו את רמת הסיכון.

בהקשר זה גם מעניין לראות כי 5 הבנקים הגדירו את הסייבר כסיכון בינוני בלבד. על החברות שהגדירו את הסייבר כאיום גבוה, נמנות 2 חברות ביטוח, 2 חברות גז ונפט, חברת אחזקות חברת תעשיה ומסחר ושירותים.





לאור כך שהסייבר הינו אחד מהסיכונים המרכזיים של ארגונים כיום, אנו סבורים שהנושא לא צריך להיות מטופל ומרוכז רק על ידי אנשי מקצוע בארגון, אלא צריך ל להוות חלק מהיבטי הניהול היום יומיים של המנהלים הבכירים בארגון וכן להוות נדבך חשוב מהנושאים העיקריים המגיעים לדיון עיתי בדירקטוריון.

אם כך, סיכון הסייבר בכל ארגון מקבל משנה תוקף בחשיבותו ומצריך כי היבטי הממשל התאגידי בניהולו יהיו ברמה גבוהה והדוקה, המותאמת כמובן לסוג הארגון, לגודלו ולאופי פעילותו, לרבות ליכולת השקעת המשאבים של הארגון. על מנת להשיג זאת חייבת להיות מעורבות גבוהה של ההנהלה הבכירה, הדירקטוריון בניהול סיכון זה והחברה צריכה לשתף את מחזיקי העניין שלה (לרבות המשקיעים) המידע הרלוונטי להם על מנת שהם יהיו סמוכים ובטוחים כי הנושא מנוהל בצורה מיטבית. זאת כמובן בהתאם להנחיות ותקנים מקובלים בארץ ובעולם ובפרט תורת ההגנה של מערך הסייבר הלאומי.

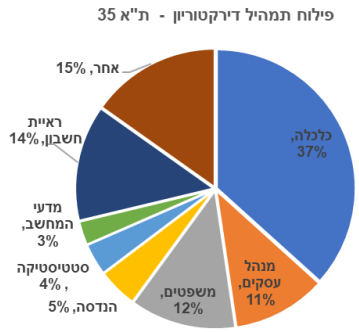
לעיתים סיכון הסייבר מגיע בדרכים מפתיעות ומאד רלוונטיות בשוק ההון. כך למשל, אנחנו עדים למקרין בהם חברות פרטיות, שלא היו מתוקשרים לפני אך מאד מתוקשרים עת החליטו לצאת להנפקה. חברות אלו העידו כי התקשור שקיבלו לאור ההנפקה השיט עליהם חשיפה נוספת של התקפות סייבר בעצימות גבוה ואשר הן לא היו ערוכים לה. כך שהן החברות והן המשקיעים נדרשים לשקול סיכון זה גם בנסיבות שכאלה.
ישנם מספר עקרונות הנדרשים ליישום על מנת להבטיח שהנושא מנוהל בצורה טובה ומקבל בכל ארגון את המשאבים הנדרשים. ראשית, נדרש שדירקטוריון החברה יהיה מעורב בנושא וזאת מתוך תפיסת Tone of the Top, אשר מייצרת אימפקט רציני בארגון, משנה ומעצבת את התרבות הארגונית שלו, לכשהדבר נדרש.
מעורבות זו מושגת בין היתר על ידי כהונה בדירקטוריון של דירקטור/ים בעל/י הבנת IT/סייבר, על ידי גיבוש מדיניות ייעודית בנושא על ידי הדירקטוריון וקיום דיון בנושא של הקצאת משאבים, באמצעות עבודה מקצועית וייעודית בועדת משנה של הדירקטוריון, בניטורו של נושא הסייבר כחלק מניהול הסיכונים בארגון, בהגברת השקיפות בארגון ומחוצה לו ולעיתים גם באמצעות שימוש ביועצים חיצוניים.
כאמור גם להנהלה חלק חשוב בתהליכים אלו שכן היא נדרשת לוודא באמצעות הכלים השונים הקיימים בארגון כי הנושא מטופל ומנותר וכי ההחלטות המתקבלות בדירקטוריון מיושמות על ידי האנשים הרלוונטים בארגון. תפקיד ההנהלה בין היתר הוא לייצר דיווחים שוטפים, לוודא את שלמות המידע וגם להרים דגלים במקרים הרלוונטיים.

בדומה לקידום היבטי ממשל תאגידי אחרים גם למשקיעים (בעיקר לגופים מוסדיים), כחלק ממחזיקי העניין, יש תפקיד חשוב בקידום הנושא על ידי החברה ובאופן טיפולו בצורה הנאותה. המשקיעים נדרשים לבחון את השקעתם, לא רק על בסיס התשואה הכלכלית הגלומה בהשקעה כנגד הסיכון, אלא גם בהיבטים נוספים שעניינם איכות הממשל התאגידי בחברה הציבורית, אשר בפועל מפחיתים את רמת הסיכון הכוללת של החברה ובתוך כך גם של השקעה.

לדוג' על משקיעים לדרוש שקיפות בנושא על מנת שיוכלו להעריך ולגבש תמונת מצב נאותה לרמת הסיכון של הארגון ולמידת השקעת המשאבים שלו בצמצום סיכון הסייבר. בנוסף עליהם לוודא כי תמהיל הדירקטוריון כולל דירקטורים בעלי ניסיון רקע בנושא, שהינם בעלי יכולת לתרום דירקטוריון בפרט ולארגון בכלל בנושא זה ובמידה ולא לפעול לכך.

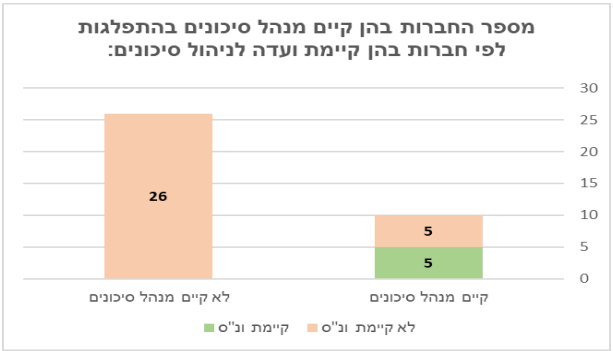
על פי תמונת מצב נוכחית של השוק ניתן לראות כי לגופים המוסדיים בישראל קיימת עבודה רבה בנושא.

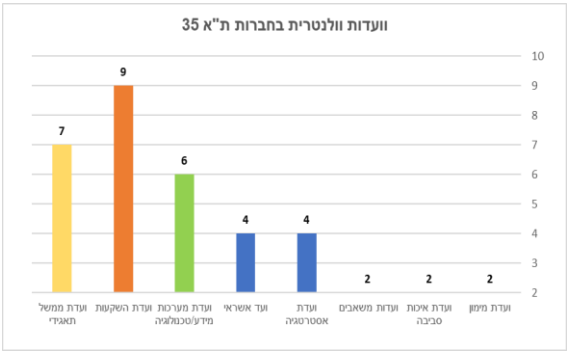
במיפוי של חברות במדד ת"א 35 (החברות הגדולות בעלות משאבים משמעותיים) ניתן לראות כי רק 3% מהדירקטורים הינם מתחומי מדעי המחשב וה IT. נתון זה לא מפתיע שכן מרבית מהדירקטורים הינם מתחומי הכלכלה, ראיית חשבון, מנהל עסקים ומשפטים ולאורך השנים היתה קיימת הטיה למינויים של דירקטורים מתחומים אלו. אנו סבורים כי קיימת חשיבות גדולה לשינוי של התמהיל ומתן ביטוי טוב יותר לדירקטורים בעלי התמחויות שונות, כגון במערכות מידע ובנושא סייבר.



מסקר שערכנו בקרב דירקטורים בחברות ציבוריות הנמנים על מאגר הדירקטורים של אנטרופי עולים הנתונים הבאים:
כ- 85% מהדירקטורים סבורים כי רמת סיכון הסייבר בארגון בו הם מכהנים הנה בינונית או גבוהה. כששאלנו את הדירקטורים לגבי כמות ואיכות הדיונים התברר כי בכ- 50% מהארגונים כלל לא מתקיים דיון בנושא סייבר בדירקטוריון החברה ובאלה שכן מתקיים מעל- 50% סבורים שכמות הדיונים אינה מספקת. כלומר, בפועל בפחות מ- 25% מהחברות מתקיימים דיונים בדירקטוריון בתדירות מספקת בנושא הסייבר.
עוד עולה מהסקר כי כ- 50% מהדירקטורים חושבים כי לדירקטוריון החברה אין את היכולת לפקח באופן יעיל ואפקטיבי על סיכון הסייבר ורק כ- 40% מהדירקטורים סבורים שהארגון שלהם משקיע משאבים מספקים להתמודדות עם סיכון הסייבר.
כשבדקנו את תוצאות הסקר עבור חברות במדד תל אביב 35 בלבד הנתונים אף החמירו והראו כי 70% מהדירקטורים סבורים כי לא מתקיימים מספיק דיונים בנושא סיכון הסייבר בדירקטוריון של החברות בו הם מכהנים, 60% מהדירקטורים סבורים כי לחברה **אין** את היכולת לפקח על סיכון הסייבר. עוד עולה כי רק כ- 30% מהדירקטורים סבורים שהארגון שלהם משקיע משאבים מספקים להתמודדות עם סיכון הסייבר.

עוד ניתן לראות כי רק ל 6 חברות מתוך חברות תל אביב 35 קיימת ועדת משנה של הדירקטוריון העוסקת בנושאים של טכנולוגיות/מערכות מידע (מתוכן 5 בנקים). מתוך אותן 36 חברות הגדולות, ניתן לראות כי רק ל- 10 חברות קיים מנהל סיכונים שהינו נושא משרה (מרביתן נמנות על ענפי הבנקים והביטוח).





למרות שזהו המצב כיום, אנו סבורים כי לגופים מוסדיים קיימת יכולת טובה לשפר היבטים אלו, שכן ראינו בשנים האחרונות כי פעולות שלהם הביאו לשיפור הממשל תאגידי בחברות הציבוריות. הדרך לעשות זאת מתחילה בהכרת

הנושא והבנת חשיבותו כחלק מניהול הסיכונים בנוסף יש לספק לגוף המוסדי (וכך גם לחברה הציבורית) כלי עבודה שיעזור לתכלל את כלל המידע הרלוונטי לנושא, בראיית משקיע בשוק ההון.

לאנטרופי קיים מודל להערכת סיכון משל תאגידי של חברות ציבוריות המשמש מזה מספר שנים את המשקיעים המוסדיים בשוק ההון בהערכת הסיכון הממשל תאגידי הגלום בהשקעתם. מודל זה מעריך את הסיכון הממשל תאגידי של כלל החברות הציבוריות וקיימים לו מספר תפקידים. ראשית המודל מהווה כלי מדידה והשוואה, ביחס לשוק ולמדד הרלוונטי וכן על פני תקופת זמן. שנית, תפקידו לייצר שיח בין המשקיעים למנפיקים בהיבט סיכון הממשל התאגידי. וכן תפקידו להוות כלי משלים למנהלי השקעות להחלטה ו/או דירוג ההשקעה גם בהיבט פוטנציאל סיכון הממשל התאגידי.

למודל קיימות 4 קטגוריות ובראשית שנת 2020 תיווסף קטגוריה ייעודית לניהול סיכונים, מערך ציות, רגולציה וסייבר, אשר תשמש את הגופים המוסדיים להערכת הסיכון של כל חברה בנושא זה (וכאמור ככלי השוואה אל מול קבוצות השוואה רלוונטיות) קטגוריה זו תהווה מודל בפני עצמו לשימוש של הארגון ככלי עבודה פנימי וזאת על מנת לבנות תוכנית עבודה ולבצע הערכות לגבי הקצאת המשאבים ויעילות התהליכים המבוצעים בארגון.