

סיכוני סייבר – ניהול ודיווח

# בעקבות פרסום ממצאי ביקורת של רשות ניירות ערך

אייל שגיא, ורד פיליכובסקי ושיר שושני-כץ | 2.2.2023

**AYR**

Amar Reiter Jeanne Shochatovitch & Co

**ACC** Association of  
Corporate Counsel  
**ISRAEL**

עמדה 105-33 :  
גילוי בנושא סייבר

**AYR**

עמר רייטר ז'אן שוכטוביץ ושות'

סיכוני סייבר – ניהול ודיווח | AYR – עמר רייטר ז'אן שוכטוביץ ושות'

המתודולוגיה ששימשה לבחינת  
מהותיות סיכוני הסייבר



קיום מדיניות סייבר ופיקוח על  
יישומה האפקטיבי



הערכות מוקדמות לטיפול  
בתקיפות סייבר



גילוי על מדיניות ניהול הסיכונים,  
החשיפה, ועל אירועי סייבר

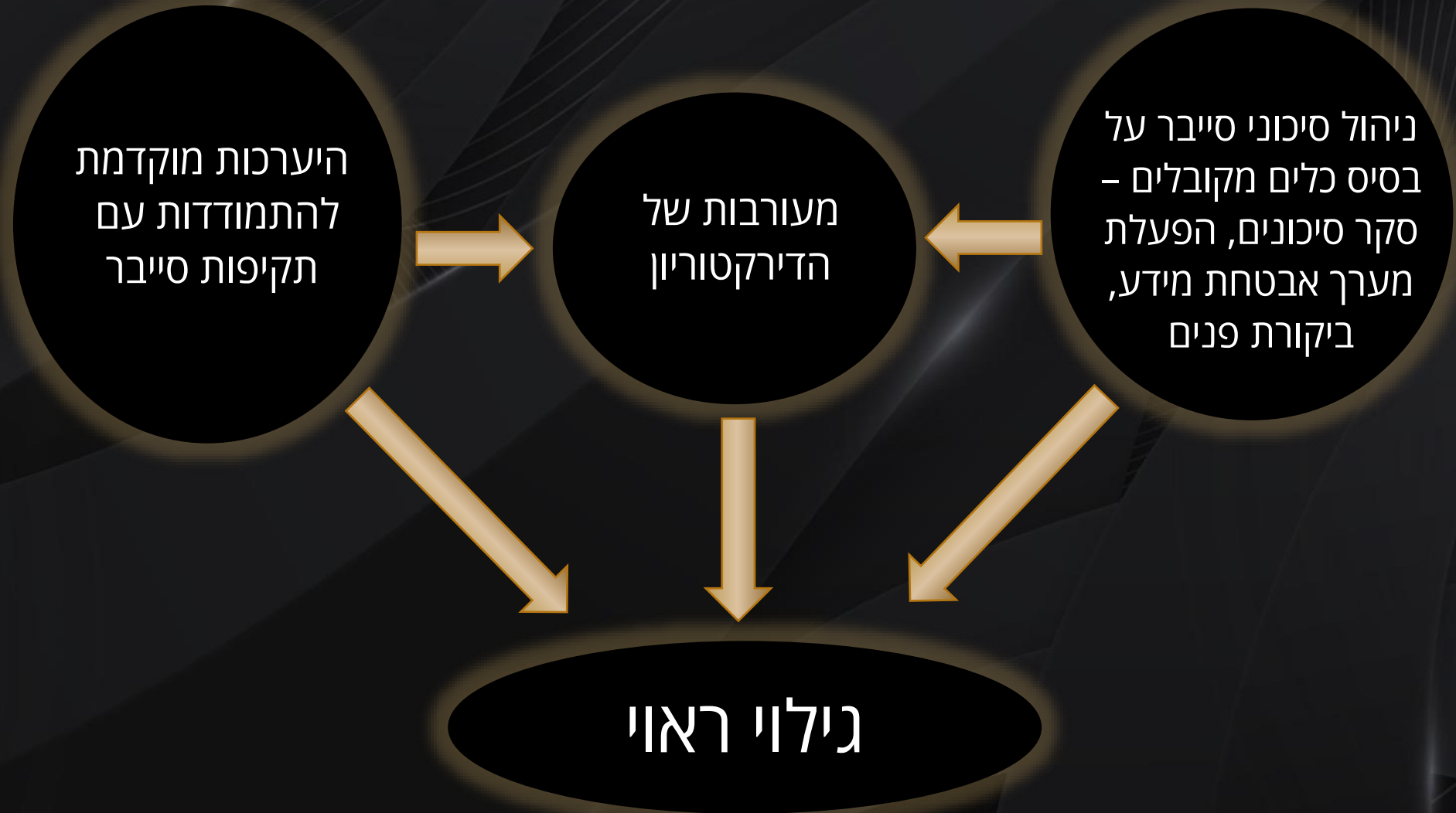


# ביקורת רשות ניירות ערך - מה נבדק?

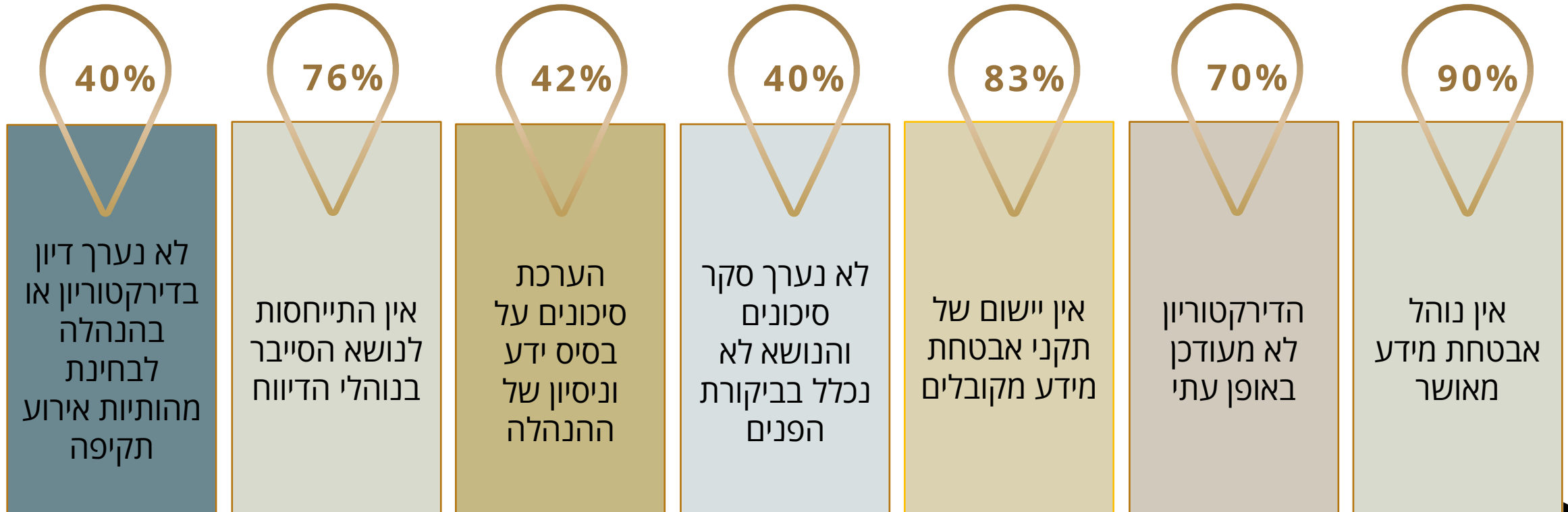
סיכוני סייבר - ניהול ודיווח | AYR - עמר רייטר ז'אן שוכטוביץ ושות'

AYR  
עמר רייטר ז'אן שוכטוביץ ושות'

# ההמלצות העיקריות



# עיקר הממצאים



רבע מחברות המדגם חוו לפחות תקיפת סייבר אחת ברמה כלשהיא בשלוש השנים האחרונות

## ניהול הסיכונים באופן שוטף

- ביצוע הערכת סיכונים באמצעות מתודולוגיה סדורה כמו 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
- עבודה לפי תכנית עבודה שנתית, שהביצוע שלה מבוקר על ידי ההנהלה
- היערכות מראש לאירוע תקיפה: בחינה של נחיצות מינוי צוות תגובה, לרבות אופיו, הרכבו, סמכויותיו והכשרתו
- קיום מערך אבטחת מידע אפקטיבי

## שילוב הדירקטוריון וההנהלה

- מעורבות משמעותית של הדירקטוריון בניהול סיכוני הסייבר של התאגיד ובהתמודדות עם אירועים
- לודא שיש ידע ומיומנות בתחום לחברי דירקטוריון או לשכור שירותים של יועצים מקצועיים לדירקטוריון
- דיווחים עתיים לדירקטוריון ודיון בישיבות הדירקטוריון בנושא: דיווחים שוטפים מאנשי הטכנולוגיה, אישורים להתקשרויות עם מיקור חוץ, דיון בהשפעת סיכוני הסייבר על התאגיד, עדכונים וייעוץ ממומחים, דיון בדבר הצורך לדווח על אירוע סייבר מהותי
- שילוב של עובדי הצד העסקי עם עובדי הטכנולוגיה

גילוי נאות

ניהול סיכון והיערכות מראש



**AYR**

עמר רייטר ז'אן שוכטוביץ ושות'

סיכוני סייבר - ניהול זדיווח | AYR - עמר רייטר ז'אן שוכטוביץ ושות'



# מקרה גולד בונד

**AYR**

עמר רייסר ז'אן שוכטוביץ ושות'

סיכוני סייבר - ניהול ודיווח | AYR - עמר רייסר ז'אן שוכטוביץ ושות'

# גילוי תקופתי – בתשקיף ובדוחות תקופתיים

גילוי על גורמי סיכון: דירוג השפעת הסיכון על החברה יתבצע בהתייחס לסיכון השיורי

פירוט אסטרטגיית ניהול הסיכונים: מתודולוגיה, נהלים, תהליכי עבודה, פעולות ובקורות, אפקטיביות

גילוי על מומחיות נושאי המשרה וחברי הדירקטוריון בתחום הסייבר

אירועי סייבר מהותיים בתקופת הדוח

דו"ח הדירקטוריון - הסברים אם החשיפה הפכה למהותית יותר או ביחס לאירוע סייבר מהותי בתקופת הדו"ח

**AYR**

עמר רייטר ז'אן שוכטוביץ ושות'

סיכוני סייבר – ניהול ודיווח | AYR – עמר רייטר ז'אן שוכטוביץ ושות'

## דיווח מיידי

קביעת נהלים ותהליכים הקשורים לחובות הדיווח של החברה:  
עיגון תהליכים לעניין גילוי בעת קרות תקיפת סייבר מהותית - מי הגורם שנדרש לדון ולהחליט?

החלטה על דיווח מיידי - בהתאם לנוהל:  
שקלול מכלול הנזק ופוטנציאל הנזק שנגרם או עלול להיגרם - במישרין ובעקיפין

בחינת המהותיות:  
בהתאם לפרמטרים כמותיים ופרמטרים איכותיים

השבתה מלאה או חלקית של הפעילות

פריצה למאגרי המידע

נזק למערכת המחזור

גניבת מידע עסקי

פריצת אבטחת מידע

דרישה לתשלום כופר

## דוגמאות



**AYR**

עמר רייטר ז'אן שוכטוביץ ושות'

# דיווחים

## • דיווח לציבור

- אירוע מהותי
- תיאור האירוע
- תיאור הנזק
- דיווחים משלימים
- דיווח מיידי

## • דיווח לרשות הגנת הפרטיות

- על "אירוע אבטחה חמור"
- חמור?
- באמצעות מילוי טופס דיווח מובנה, ומפורט
- אפשרות של דיווח לנושאי המידע
- מיידי, באמת



יכול להיות דיווח רק במסגרת דיני ניירות ערך / במסגרת דיני הגנת הפרטיות / כפול / משולש

- תוכן (מידע אישי)
- רף
- נוהל

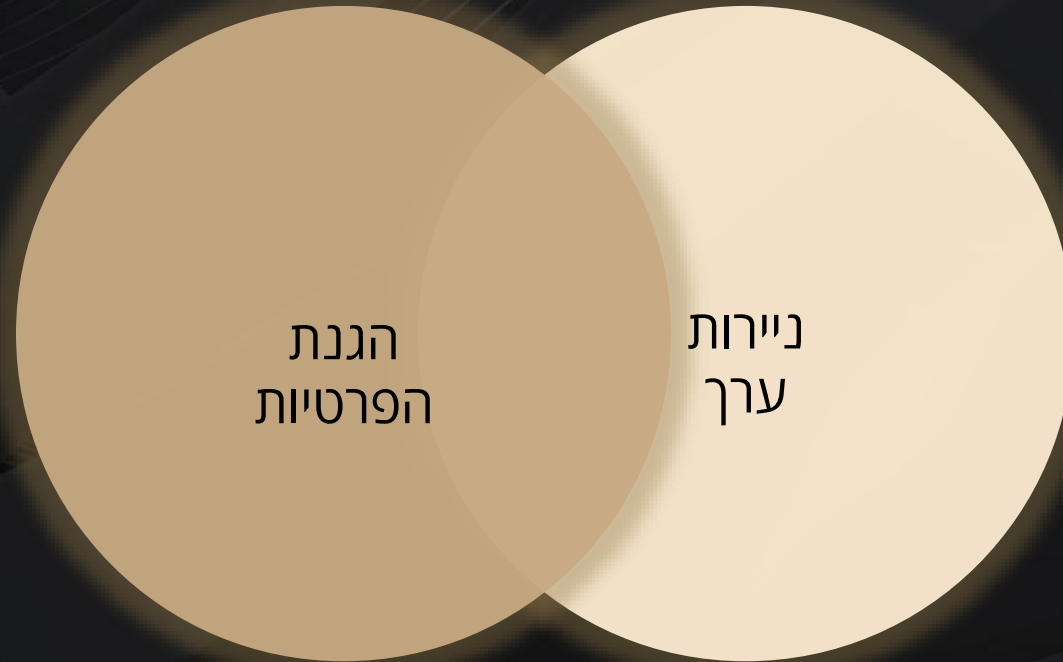
# המלצות ליישום

הגנת הפרטיות	תאגיז מדווח	
אין התייחסות ספציפית, כי מדובר בדין כללי	להבטיח ידע ומיומנות בדירקטוריון	הרכב הדירקטוריון
ברמה גבוהה – סקר סיכונים אחת ל 18 חודשים	באמצעות מתודולוגיה סדורה	הערכת סיכונים
ברמה בינונית – דיון באירועי אבטחה ובעדכון נוהל האבטחה, אחת לשנה לפחות; ברמה גבוהה – אחת לרבעון, ויש חובות לדון גם בתוצאות סקר סיכונים, מבדקי חדירות ודוח הביקורת	שוטף, תקופתי	דיון תקופתי בדירקטוריון
	מומחים בסייבר/אבטחת מידע	יועצים

# המלצות ליישום - המשך

הגנת הפרטיות	תאגיד מדווח	
ממונה אבטחת מידע חב בבניית "תכנית בקרה". ככלל, מומלץ לערוך תכנית עבודה שנתית בהגנת הפרטיות ואבטחת מידע	תכנית עבודה שנתית, בקרה של ההנהלה על יישומה	תכנית עבודה
ברמה בינונית או גבוהה – ביקורת חיצונית או פנימית אחת ל-24 חודשים לפחות	לכלול נושאים של סיכוני סייבר ואבטחת מידע	ביקורת פנים
נדרש כחלק מתוכן נוהל האבטחה	קביעת נהלים להתמודדות עם תקיפה ולדיווח על האירוע	הערכות לאירוע תקיפה
כשמדובר ב"אירוע אבטחה חמור", דיווח מייד	בחינת מהותיות לפי פרמטרים איכותיים וכמותיים	דיווח מייד

# מסקנות עיקריות



דיונים, נהלים, מתודולוגיה, תוכנית עבודה, תוכנית בקרה, תיעוד, דיווחים, אבטחת מידע, עדכוני תוכנה, מיקור חוץ, מודעות עובדים, הדרכות, סקרים, ביקורות





# THANK YOU

**AYR**

עמר רייטר ז'אן שוכסוביץ ושות'



**שיר שושני-כץ**  
מנהלת מחלקת  
משפט וטכנולוגיה  
[ShirS@ayr.co.il](mailto:ShirS@ayr.co.il)



**ורד פיליכובסקי**  
ראש מחלקת שוק ההון  
וניירות ערך  
[VeredPi@ayr.co.il](mailto:VeredPi@ayr.co.il)



**אייל שגיא**  
ראש מחלקת  
משפט וטכנולוגיה  
[EyalS@ayr.co.il](mailto:EyalS@ayr.co.il)