לשכת המבקרים הפנימיים IIA ישראל (חל"צ)
IIA Israel - Institute of Internal Auditors

הכנס המקצועי השנתי של הביקורת הפנימית 2026

Internal Audit NextGen2.0

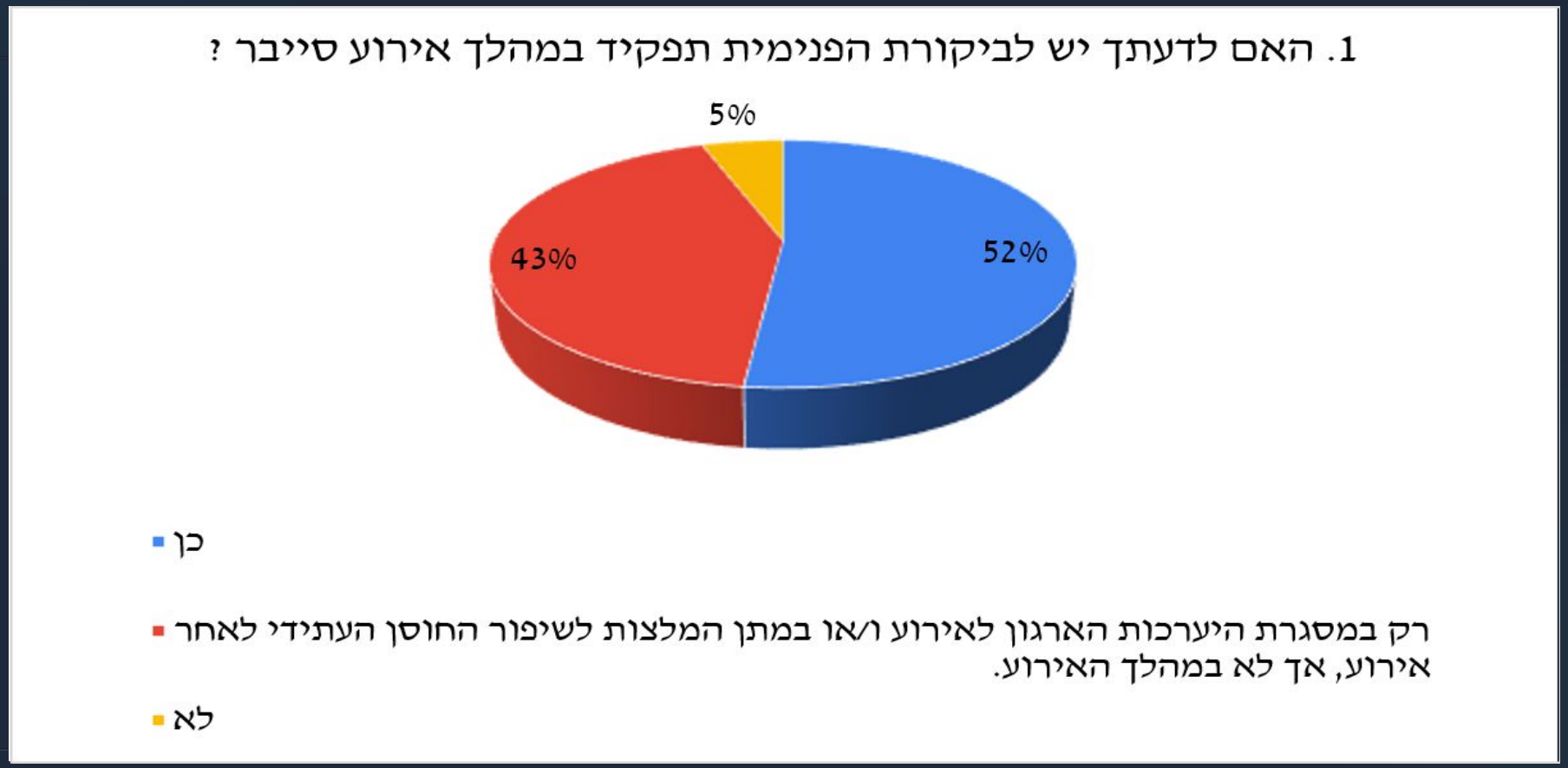
מעורבות הביקורת
באירוע סייבר

אלון עמית - הנשיא שקדם איגוד ISACA ישראל, משרד רו"ח רווה רביד

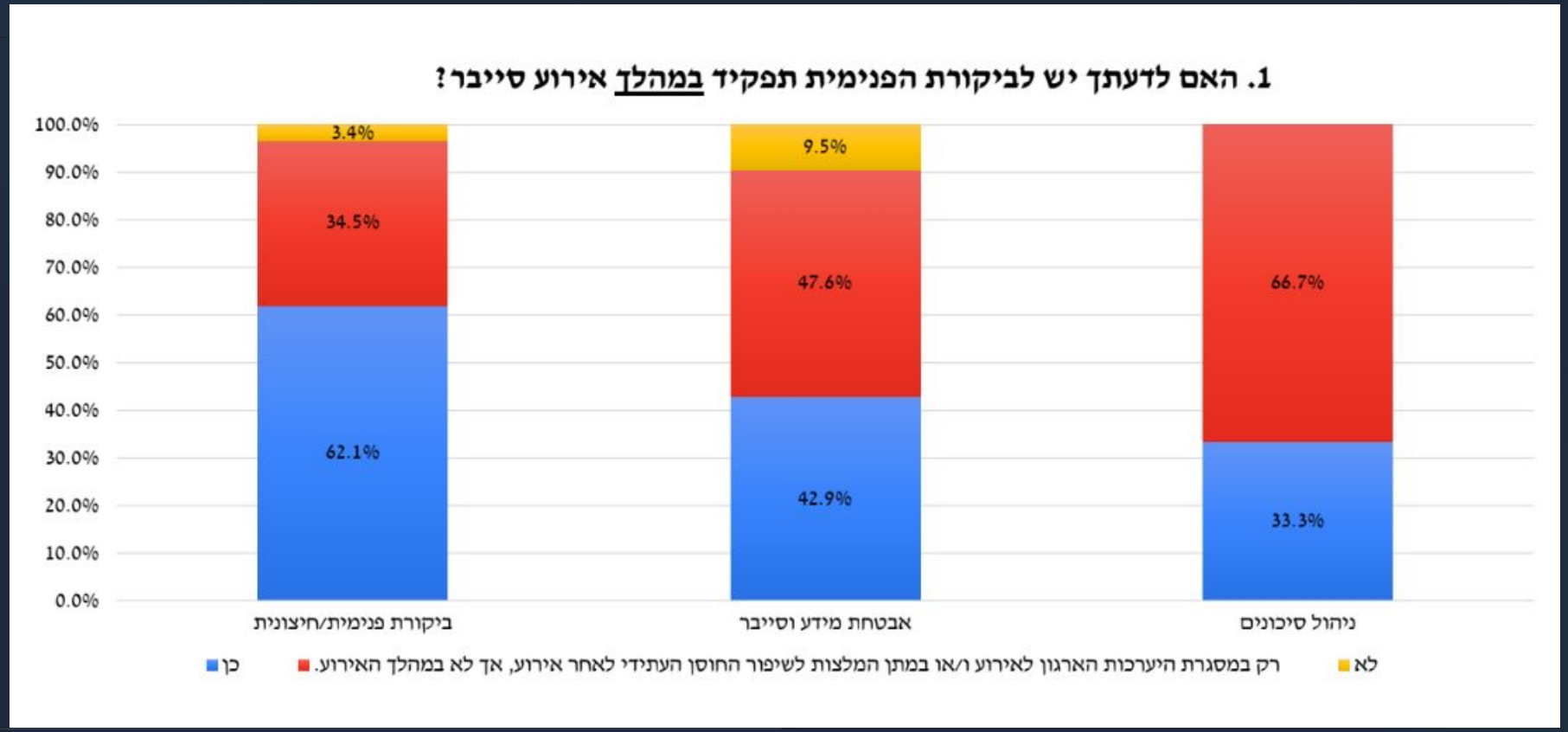
בר וויס סלהוב- סגנית נשיא ויו"ר הועדה המקצועית איגוד ISACA ישראל, מבקרת פנים ראשית- בנק אש ישראל

מבוסס על נייר עמדה של הוועדה המקצועית - איגוד ISACA ישראל

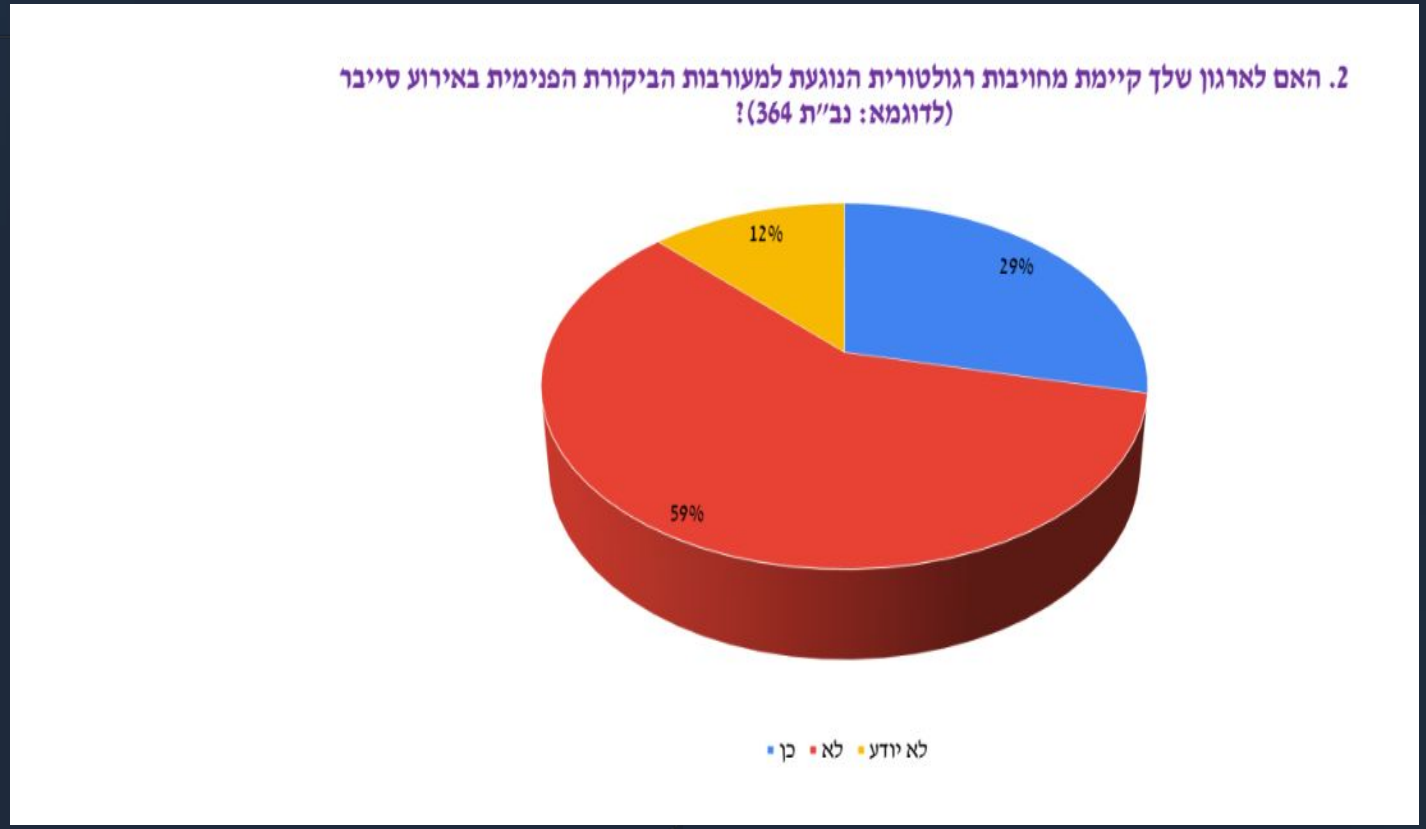
תפקיד הביקורת באירוע סייבר – מה חושבים המבקרים ,אנשי אבטחת מידע ומנהלי סיכונים?



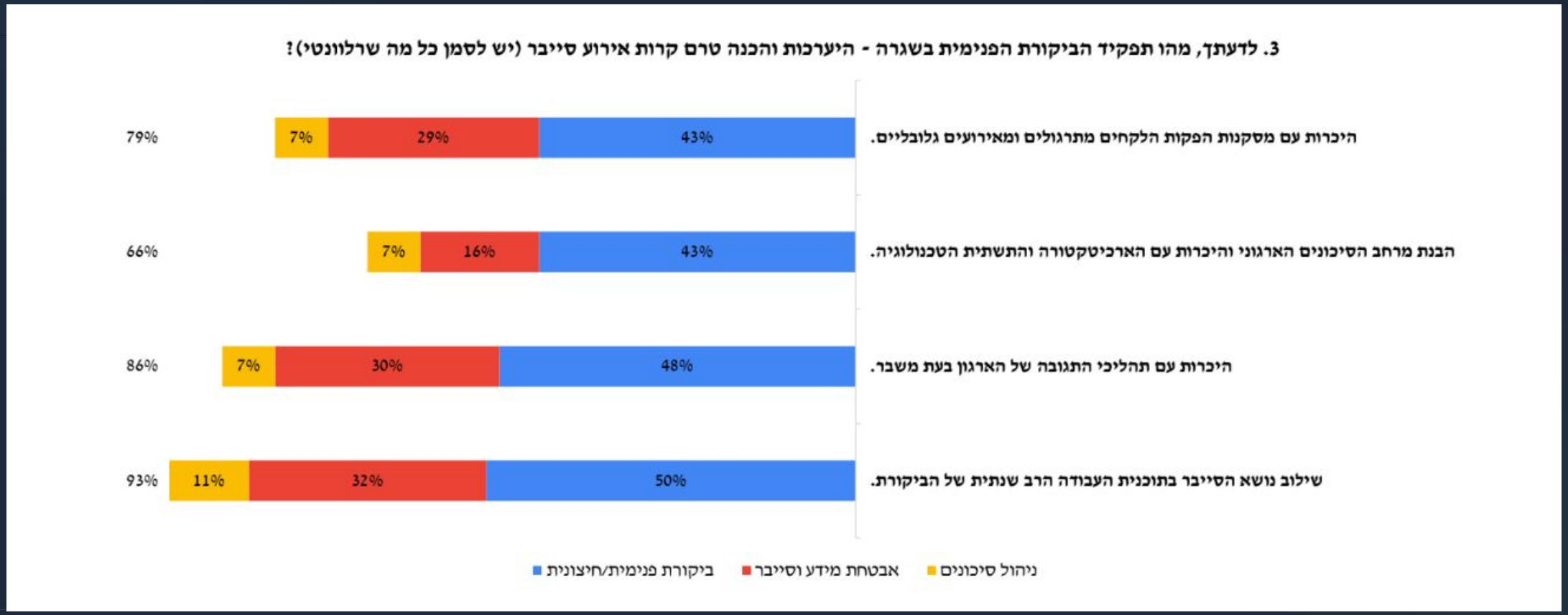
תפקיד הביקורת באירוע סייבר – מה חושבים המבקרים, אנשי אבטחת מידע ומנהלי סיכונים?



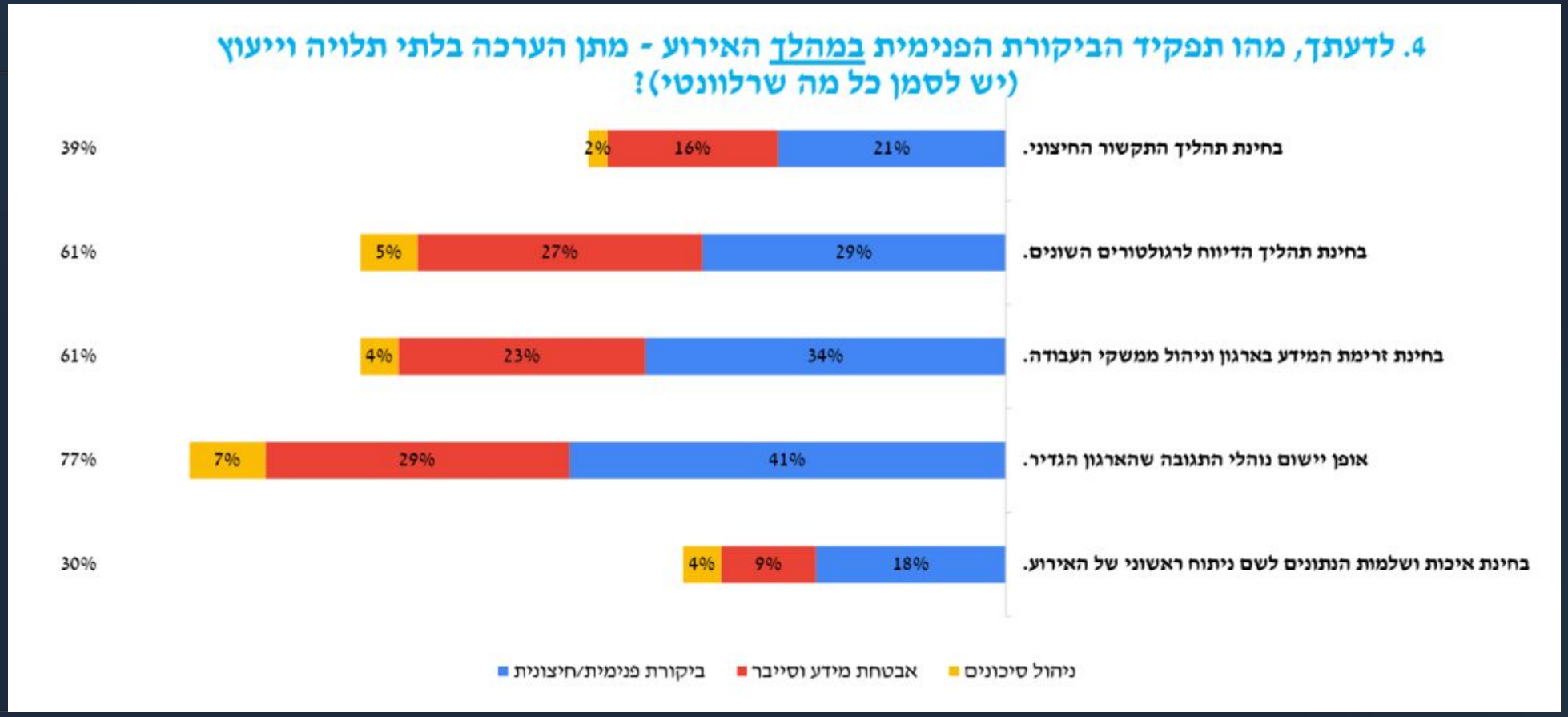
תפקיד הביקורת באירוע סייבר – מה חושבים המבקרים ,אנשי אבטחת מידע וניהול סיכונים?



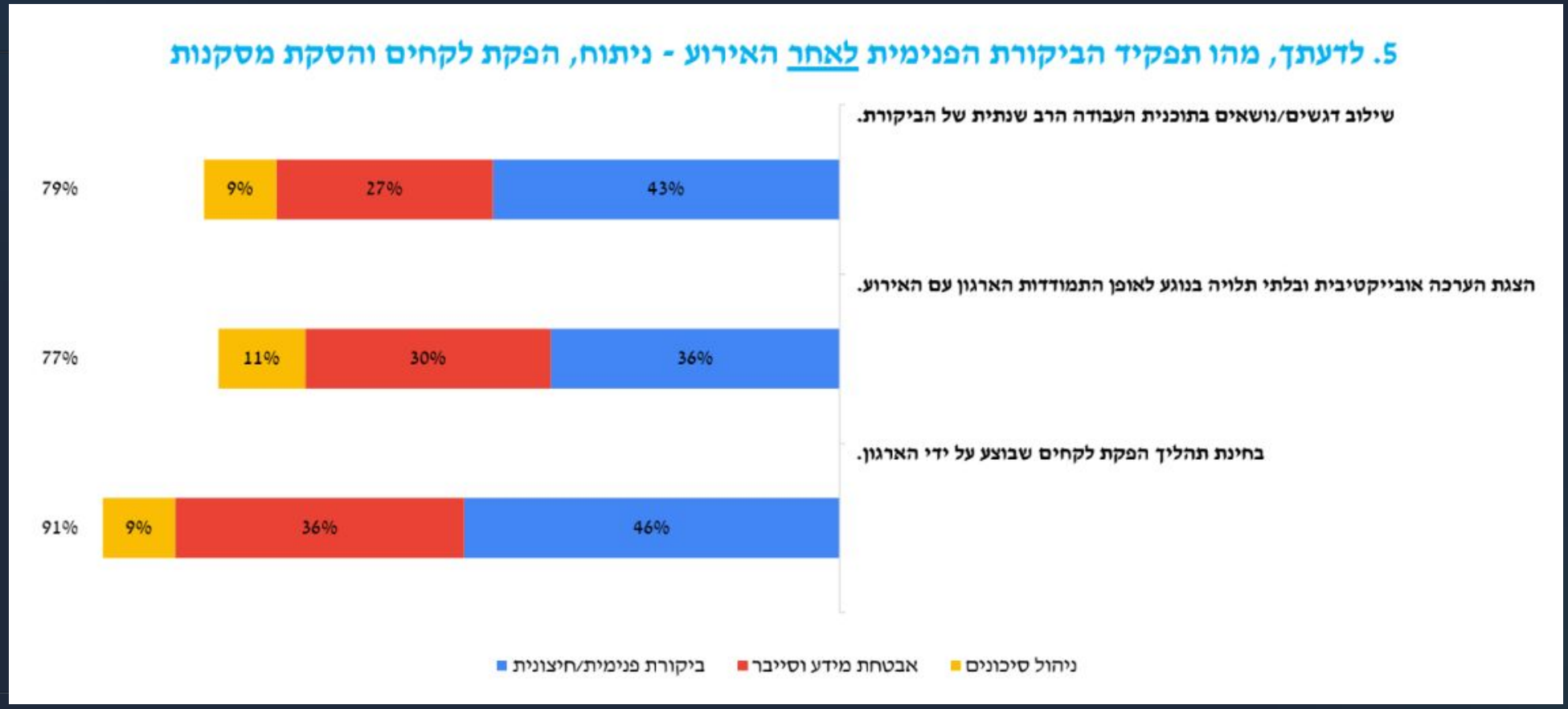
תפקיד הביקורת באירוע סייבר – מה חושבים המבקרים,אנשי אבטחת מידע ומנהלי סיכונים?



תפקיד הביקורת באירוע סייבר – מה חושבים המבקרים, אנשי אבטחת מידע ומנהלי סיכונים?



תפקיד הביקורת באירוע סייבר – מה חושבים המבקרים, אנשי אבטחת מידע ומנהלי סיכונים?



איך הכל התחיל?

נב"ת 364 בנושא "ניהול סיכוני טכנולוגיית המידע, א"מ והגנת הסייבר"

"...לצורך ביצוע ביקורות בזמן אמת בתחום טכנולוגיית המידע, אבטחת המידע והגנת הסייבר, על הביקורת הפנימית לקבוע מתודולוגיה שתתייחס בין היתר: להגדרת אופן מעורבותה בזמן אמת בתהליך לניהול אירועים ובעיות שקבע התאגיד הבנקאי ..."(סעיף 39)

ISACA Task Force - צוות החשיבה

בר וויס סלהוב

מבקרת פנים ראשית

בנק אש ישראל

דר' אלון כהן

מרצה וחוקר בתחומי הביקורת - אוניברסיטת אריאל

ברק ז'אן

ראש תחום ביקורת סייבר- בנק דיסקונט

סמדר דברת

מבקרת פנים ראשית

קופ"ח מאוחדת

מדוע נדרשת מעורבות ביקורת באירוע סייבר?

- **סיכון מרכזי:** הסייבר הוא אחד הסיכונים המשמעותיים ביותר בפעילות הארגון כיום.
- **הרחבת התפקיד:** תפקיד הביקורת השתנה והתרחב לאור התקנים המקצועיים החדשים (המבקר כיועץ אטסרטגי).
- **רגולציה (נב"ת 364):** דרישה מפורשת מבנק ישראל להגדיר את אופן מעורבות הביקורת בזמן אמת בתהליך לניהול אירועים.

דגשים לפעילות המבקר - ציר הזמן
מתי אנחנו נכנסים לתמונה

טרום אירוע	בעת אירוע	לאחר אירוע
היערכות והכנה בשגרה	הערכה וייעוץ בזמן אמת	ניתוח והפקת לקחים

שלב 1: בשגרה - בונים את החוסן הארגוני

תכנון ומוכנות

- שילוב נושא הסייבר בתכנית העבודה הרב-שנתית של הביקורת.
- היכרות מעמיקה עם תהליכי התגובה של הארגון בעת משבר (IRP).

למידה וניתוח

- הבנת מרחב הסיכונים הארגוני והיכרות עם הארכיטקטורה והתשתית הטכנולוגית.
- למידה ממסקנות הפקות לקחים מתרגולים ואירועים גלובליים.

הביקורת מהווה חלק מהחוסן הארגוני ולכן עליה להיערך לקראת אירוע סייבר

שלב 2: בזמן אמת - האיזון העדין

אירוע סייבר הוא "מבחן חוסן" (Resilience Test) לארגון כולו.

המטרה והאתגר שלנו: לספק תמונת מצב אובייקטיבית ובלתי תלויה, לאתגר את ההחלטות ולהציג נקודות מבט חלופיות שעשויות לחשוף "עיוורון" ארגוני, **מבלי** להפוך לנטל על הצוותים המנהלים את האירוע.

המבקר נדרש להפעיל שיקול דעת בנוגע לאופן מימוש מעורבות בשלב זה.

שלב 2: העיניים שלנו בשטח: מה בודקים ב"זמן אש"?

איכות ושלמות הנתונים

בחינת איכות המידע שמגיע למקבלי ההחלטות. האם זוהו התהליכים והמערכות שנפגעו והשפעתם על הארגון?

פעילות בהתאם לנהלים

האם פועלים לפי ה-Playbook שהוגדר? במידה ויש חריגה (וזה קורה) מהם השיקולים והאם מאושר ע"י הנהלה ומדווח לדירקטוריון

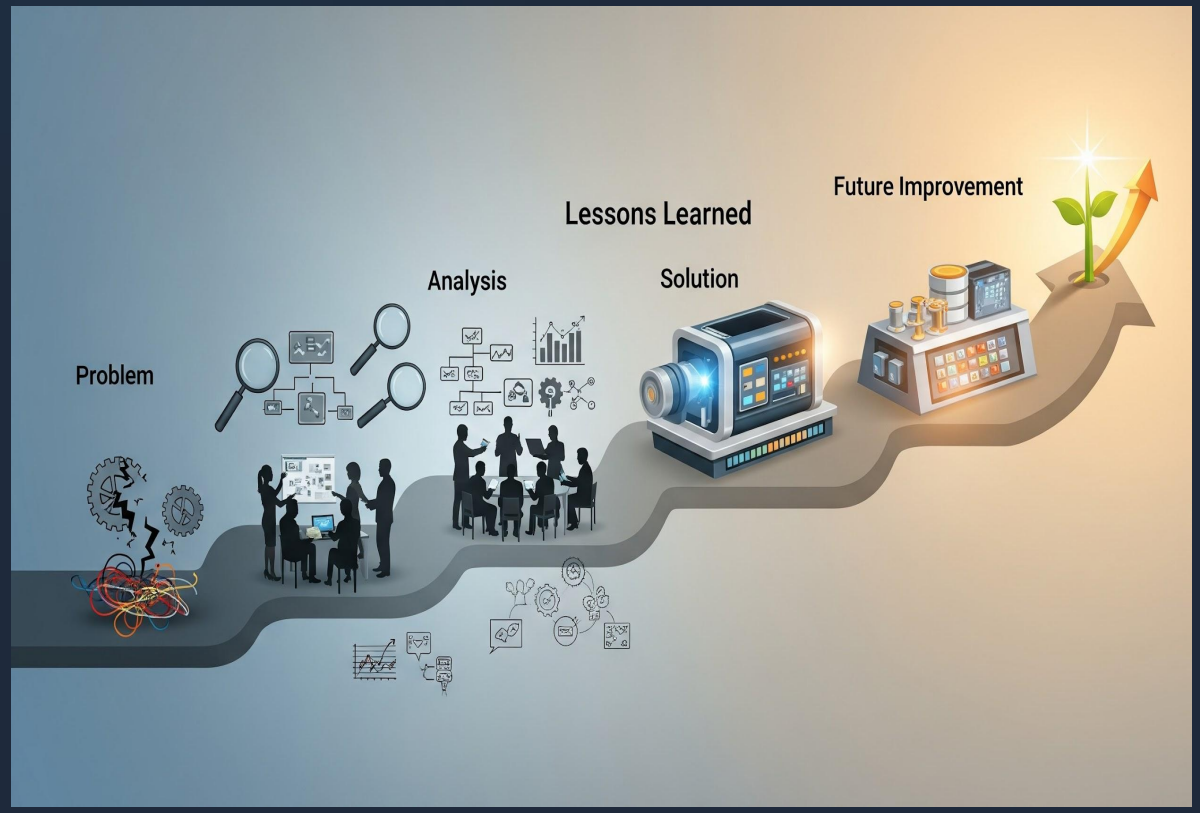
חשוב להקפיד על ניהול יומן אירועים (Log) מדויק בזמן אמת.

שלב 2 : ניהול האירוע הוא לא רק טכנולוגי

בחינת ממשקים רוחביים

- **זרימת מידע וניהול ממשקים**: מעורבות הגורמים הרלוונטיים, קיומם של דיווחים סטטוס שוטפים כולל דירקטוריון.
- **דיווח לרגולטור**: וידוא עמידה בחובות הדיווח ובמועד.
- **תקשורת ודוברות:** האם המסרים לציבור וללקוחות אחידים ומדויקים?
- **זיהוי סיכונים רוחביים נגזרים** - משפטי,מוניטין, פיננסיים וכד'.

שלב 3:לאחר האירוע - ניתוח והפקת לקחים



- **בחינת התחקיר**: הערכת תהליך הפקת הלקחים שבוצע על ידי הארגון - האם הוא שורשי ומקיף?
- **הערכה אובייקטיבית**: הצגת דוח בלתי תלוי על אופן התמודדות הארגון עם האירוע.
- **מבט קדימה**: שילוב הדגשים שעלו בתכנית העבודה הרב-שנתית לשיפור החוסן העתידי.

תובנות ומחשבות להמשך

תיאום ציפיות

הגדירו מעורבות מראש

בהתאם לציפיות הדירקטוריון

ארגז כלים

הכינו כלי עבודה ומתודולוגיה

מותאמים לארוע סייבר

אימון

תירגול שוטף הוא המפתח

להצלחה בזמן אמת

תודה על ההקשבה

קישור לנייר העמדה


INTERNAL
AUDIT
CYBER ATTACK
SECURITY BREACH