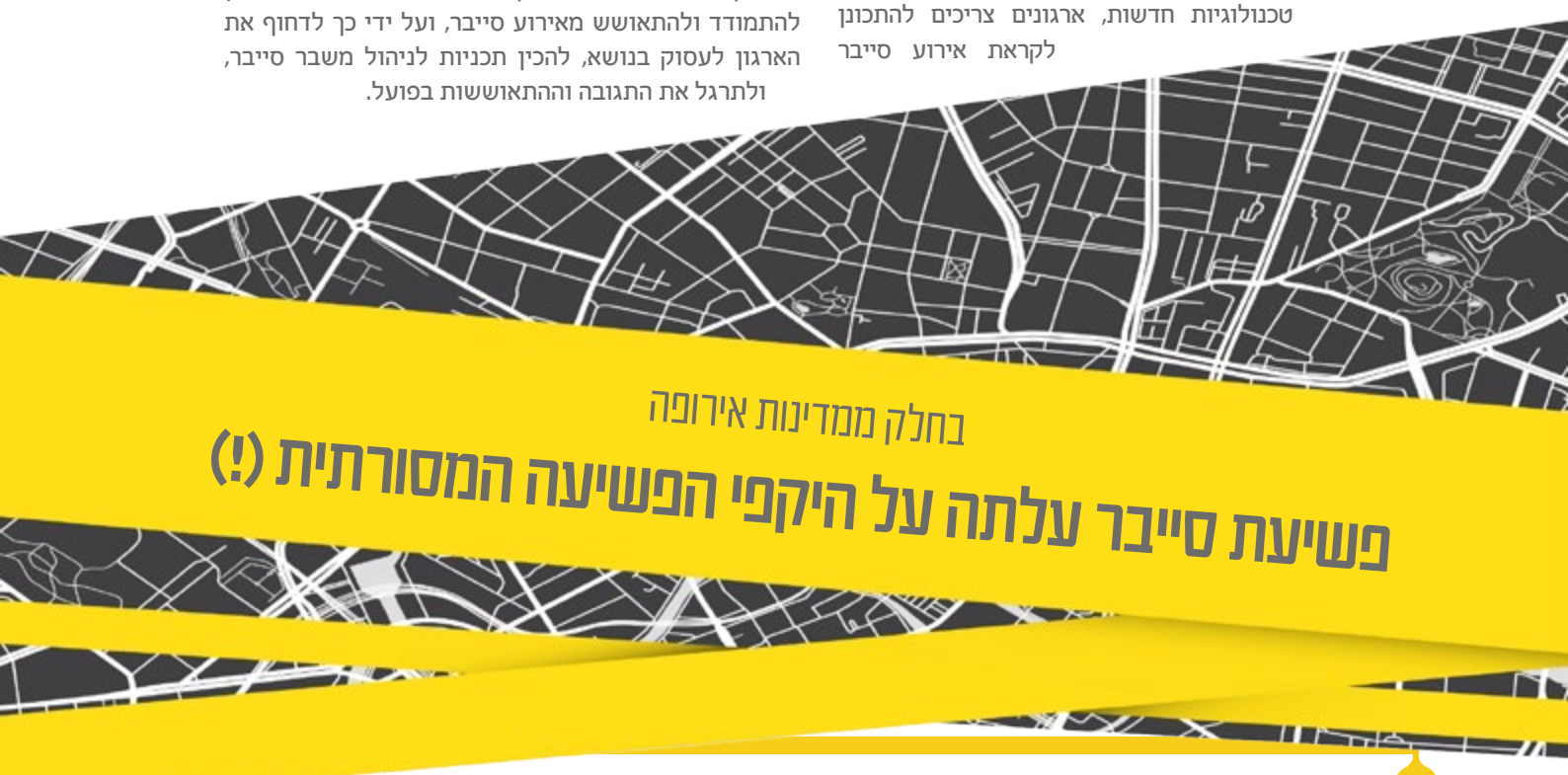
להיות חכם, ולא רק צודק: היערכות ארגונים למתקפת סייבר

מאת **אלי זילברמן כספי**

כמות תקיפות הסייבר ומורכבותן הולכות וגדלות ובקצב גבוה. עד כמה המגמה הזו משמעותית? שימו לב לנתון הבא: בחלק ממדינות אירופה פשיעת סייבר עלתה על היקפי הפשיעה המסורתית(!) כך על פי דוח של האינטרפול מספטמבר 2016. לאור מגמות עולמיות אלו, יש לקחת בחשבון שיהיה קשה מאוד לזהות ולעצור חלק מתקיפות אלו, זאת על פי המלצות המדריך של NIST 800-184 העוסק בהתאוששות מאירוע סייבר (Guide for Cybersecurity Event Recovery), שפורסם בדצמבר 2016. על פי מדריך זה, התמקדות אך ורק במניעת תקיפות סייבר אינה מספקת, ולצד שיפור יכולות ההגנה ואימוץ טכנולוגיות חדשות, ארגונים צריכים להתכונן לקראת אירוע סייבר ולשפר את יכולת התגובה וההתאוששות שלהם. היערכות מוקדמת להתמודדות והתאוששות מאירוע סייבר עשויה לצמצם משמעותית נזקים פוטנציאליים.

מצד שני, אי הכנה ותגובה מהוססת או לא נכונה, עלולה להכניס את הארגון לסחרור מסוכן. עם זאת, ארגונים רבים נמנעים מלהכין את עצמם לניהול אירוע סייבר וההתאוששות ממנו, ומעדיפים להשאיר את הנושא על כתפיו (הרחבות אך לא מספיקות) של מנהל הגנת הסייבר והכוונתו להמשיך בבניית יכולות ההגנה. על כן, קיימת חשיבות מיוחדת שהביקורת הפנימית תעסוק גם בבחינת מוכנות הארגון להתמודד ולהתאושש מאירוע סייבר, ועל ידי כך לדחוף את הארגון לעסוק בנושא, להכין תכניות לניהול משבר סייבר, ולתרגל את התגובה וההתאוששות בפועל.



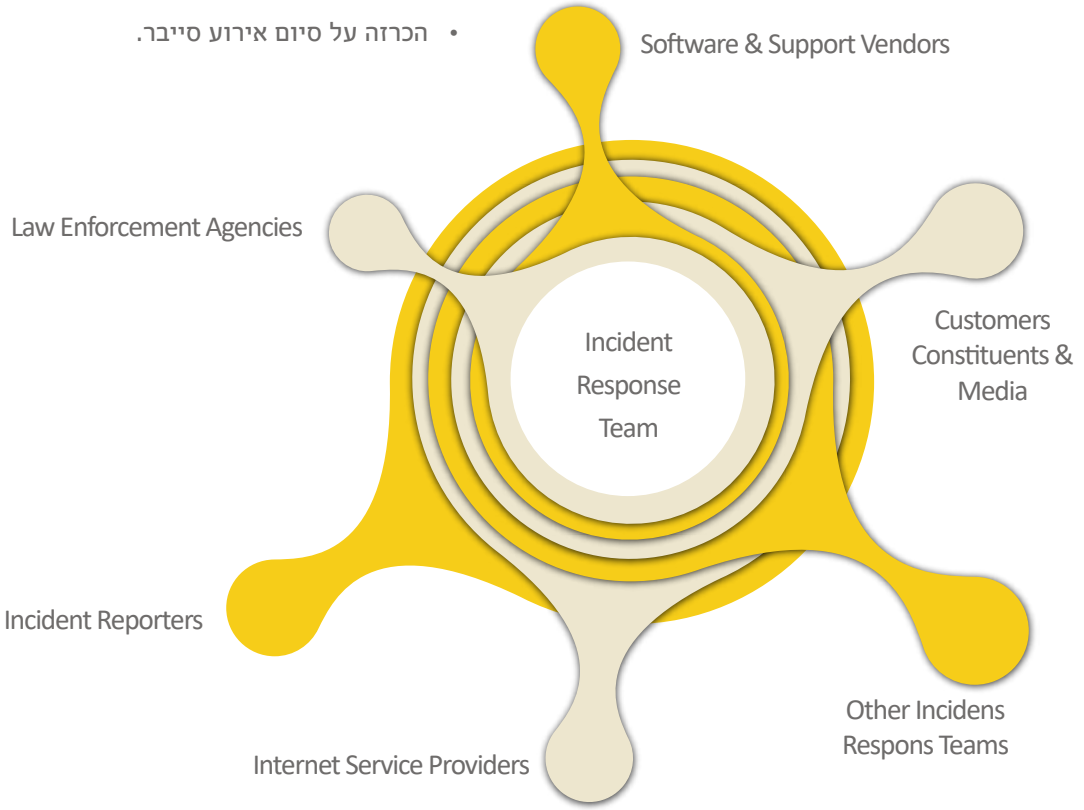
תכנית לניהול משבר סייבר מטרתה ותכולתה

תכנית ניהול משבר סייבר צריכה לשקף הסכמה של הארגון בנוגע לאופן שבו יפעל בזמן אירוע סייבר. מסגרת זו תגדיר חלוקת אחריות ברורה בין כלל הגורמים הרלוונטיים, כלומר מנהלים בכירים, מנהלי הסיכונים, היועצים המשפטיים, הצוותים הטכניים (רשת, תקשורת, אפליקציות, DBA, אבטחת מידע וכו'), אנשי יחסי הציבור והדוברות, יועצי ניהול משבר, מו"מ ועוד.

לאור סביבת חוסר הוודאות הרבה שתשרור בזמן אירוע ולאור ההבדלים (לפעמים אף גדולים) בגישות, הצרכים והאינטרסים של השותפים השונים בצוות ניהול האירוע, שיתוף הפעולה הנכון בין הגורמים הללו אינו טריוויאלי בכלל. לכן מעורבות כלל הגורמים בגיבוש התכנית הוא קריטי ליכולת שלהם לפעול בצורה נאותה בזמן אירוע. בסופו של תהליך, התכנית תשקף באופן פורמלי וממוקד את גישת הארגון לניהול אירועי סייבר.

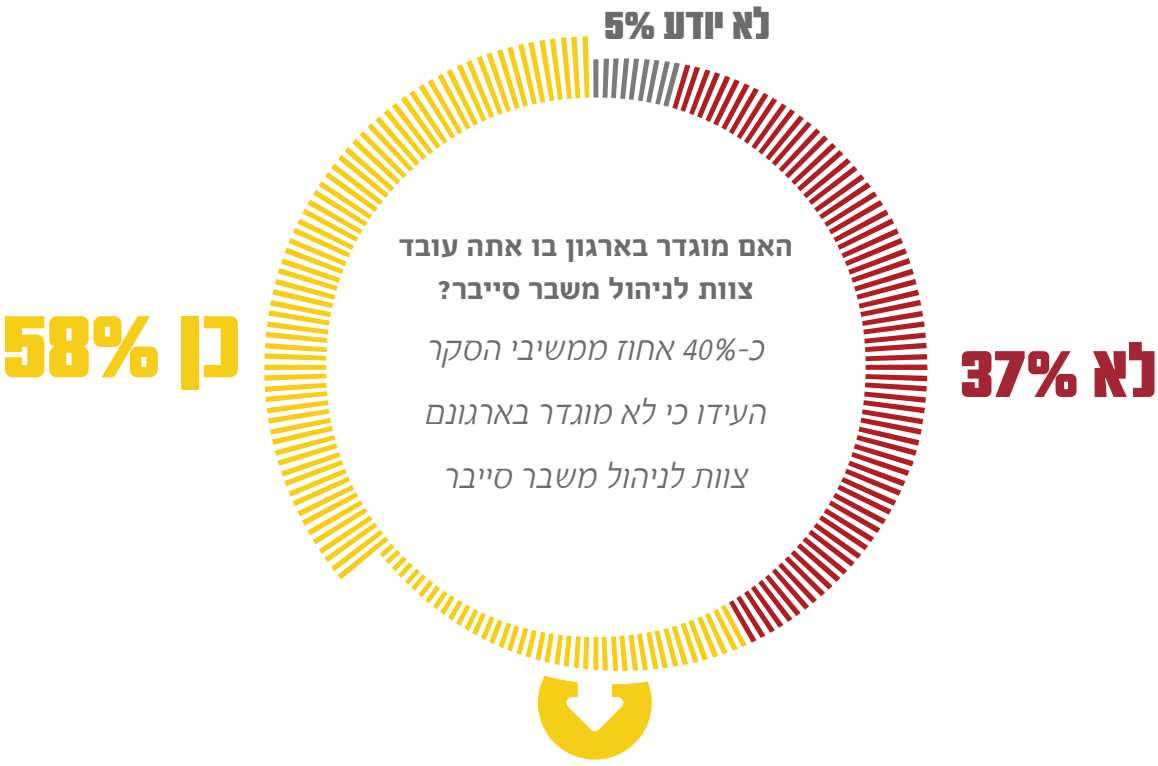
על התכנית לספק מפת הדרכים ברורה לניהול האירוע, כאשר היא נותנת מענה לדרישות הייחודיות של הארגון, לוקחת בחשבון את האסטרטגיה העסקית, גודל הארגון, המבנה והפונקציות השונות. התכנית תכלול בין היתר התייחסות לנושאים הבאים:

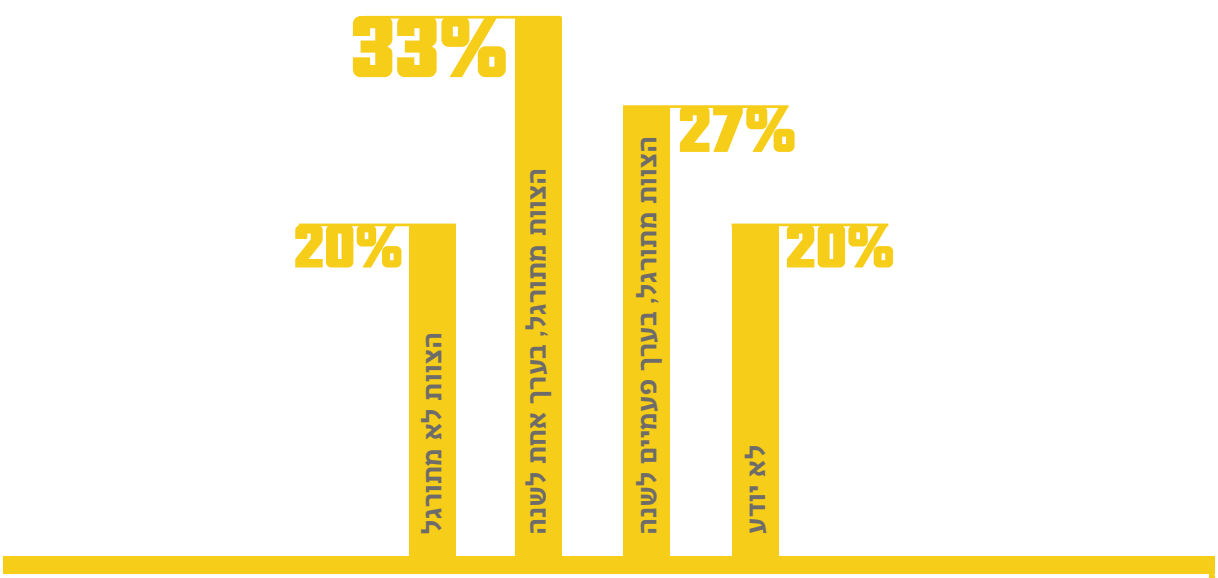
- עקרונות הכוננות לאירוע סייבר, ההכרזה על אירוע סייבר והגדרת רמת האירוע.
- מבנה ואיוש חדרי מצב.
- דרכי תקשורת.
- גופים ותהליכי עבודה ייעודיים לניהול אירוע בסייבר (חדרי מצב).
- אופן ביצוע הערכת מצב ועקרונות הדיווח לבעלי עניין.
- הפעולות הנדרשות בשלבי ניהול האירוע (מזיהוי ועד להתאוששות) - טכנולוגי, עסקי, משפטי, מוניטיני.
- עקרונות לניהול מו"מ במסגרת אירוע סייבר.
- הסתייעות בגורמים ממשלתיים ועבודה מול רגולטורים ורשויות החוק בארץ ובעולם.
- פעילות בתחום המוניטין והתקשורת.
- טבלת כוננויות וכשירויות.
- הכרזה על סיום אירוע סייבר.



להלן נתון שצריך לשים אליו לב - בישראל, כרבע מהארגונים סבלו ממתקפת סייבר בעלת השלכות על הפעילות השוטפת במהלך שלוש השנים האחרונות, כך עולה מסקר ארצי שערכנו יחד עם דלויט ואיגוד האינטרנט הישראלי. בסקר השתתפו 150 מנהלי אבטחת מידע, מערכות מידע ומנהלי סיכונים, רובם מהמגזר הפיננסי, מההיי-טק ומגופים ממשלתיים.

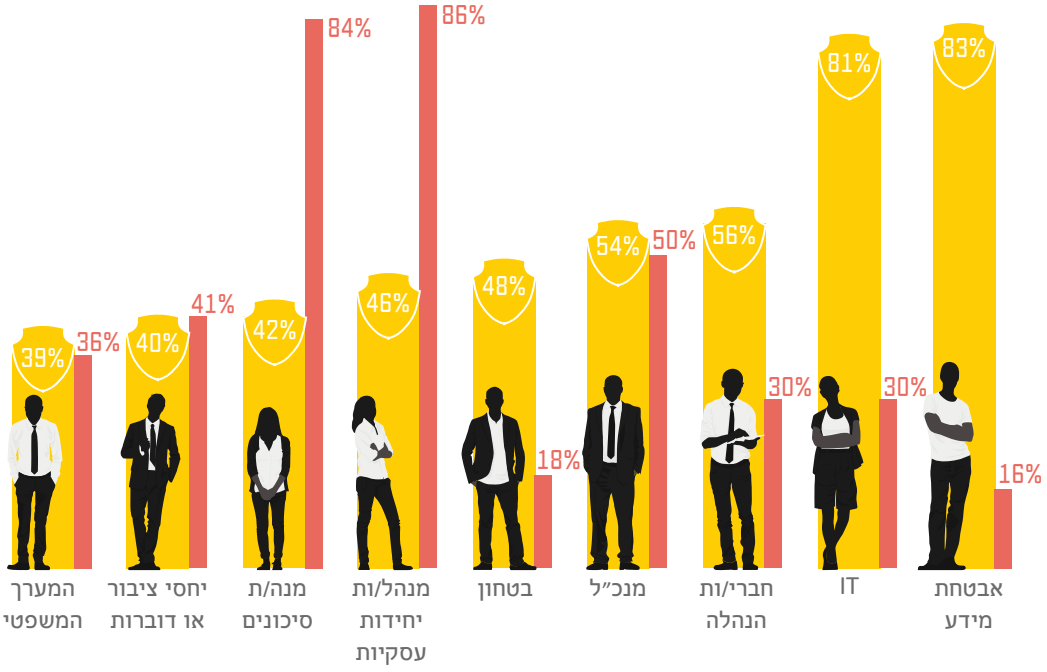
כ-40% אחוז ממשיבי הסקר העידו כי לא קיים בארגונם צוות לניהול משבר סייבר. יתר על כן, כ-20% מצוותי התגובה לא תורגלו מעולם.





בנוסף, ביותר מחצי מצוותי התגובה אין בעלי תפקידים הכרחיים, כגון מנהלים עסקיים, מנהלי סיכונים, דוברים, גורמים משפטיים וכו'.

מי הגורמים החברים בצוות ניהול משבר סייבר והאם תורגלו בשנתיים האחרונות?



ניתן ללמוד מתוך הוראת ניהול בנקאי תקין 361 בנושא ניהול הגנת הסייבר , על חשיבות ראייה כלל ארגונית באיוש צוות התגובה לצורך התמודדות נכונה עם אירוע סייבר.

על פי סעיף 76 להוראה:

"לצורך ניהול אירוע סייבר יקים התאגיד הבנקאי חדר מצב, ויגדיר בראיה משולבת כלל-תאגידית, את קבוצת העובדים אשר יאיישו אותו, את תפקידיהם, סמכויותיהם, גורמי דיווח פנימיים וחיצוניים, דרכי תקשורת, כלי עבודה וכן נוהלי עבודה פרטניים".

לתרגל או לא לתרגל - זאת השאלה

הדבר הראשון שחשוב להבין הוא כי בעת אירוע סייבר, מתמודד הצוות הטכנולוגי של הארגון עם חוסר ודאות. תוקפים מיומנים יבצעו פעולות הטעיה, כך שלעתים יכול לעבור זמן רב עד שתאותר הבעיה האמיתית. השלבים הראשונים של הטיפול באירוע מתאפיינים בחוסר מידע - מה בדיוק קרה, מה הנזקים, מי התוקף ומה הוא רצה. לאור זאת, הארגון עלול להיתפס במצב של הפתעה, ואי מוכנות לפעולה בסביבת אי ודאות שכזו שעשויה להשפיע על היכולת של מנהלים להוביל את הארגון בשעת משבר. בתוך סביבת חוסר הוודאות הטכנולוגית, הארגון חשוף לסיכונים עסקיים, משפטיים וכמובן סיכון לפגיעה במוניטין. על כן, תגובת הארגון היא קריטית ומצריכה שלל החלטות שאמורות להתבצע בשלב הזה באופן מהיר: איזה מסר מעבירים ללקוחות, לעובדים, לרשויות, לתקשורת; מה לוחות הזמנים, וכמובן מה מותר או אסור לעשות וכו'.

אחת הדרכים האפקטיביות ביותר לבחינת המוכנות הארגונית להתמודדות עם אירוע סייבר היא בעזרת סימולציה המדמה תקיפת סייבר. הסימולציה היא כלי יעיל במיוחד לביקורת, משום שהיא מאפשרת למפות את הפערים בין התכנון לביצוע ואת מכלול הפעולות שנעשו על מנת להגיב נכון בזמן אמת. סימולציה מתאימה תוכל לבחון את יכולת החברה לזהות ולהגיב למתקפות סייבר על פי וקטורים רלוונטיים לארגון, ולבדוק את כשירות הארגון ותהליך קבלת ההחלטות תחת אירוע סייבר. דרך אפקטיבית נוספת היא דיוני "What If". בדיונים אלה מעלים לדיון תרחיש סייבר שקרה בארגון דומה בארץ או בעולם, ומנתחים את ההשלכות של אירוע זה אילו היה קורה בארגון המתורגל. דיונים מסוג זה מעלים תובנות בעלות ערך רב בנוגע לרמת ההיערכות ואילו בקרות נוספו יש לממש, וכן ליכולת ולתהליך ניהול המשבר.

דוגמה בולטת להיערכות לא מספקת ותגובה לא נכונה היא של חברת Talk Talk, ספקית התקשורת השנייה בגודלה באנגליה, שחוותה מתקפת סייבר משולבת ב-21 באוקטובר 2015.

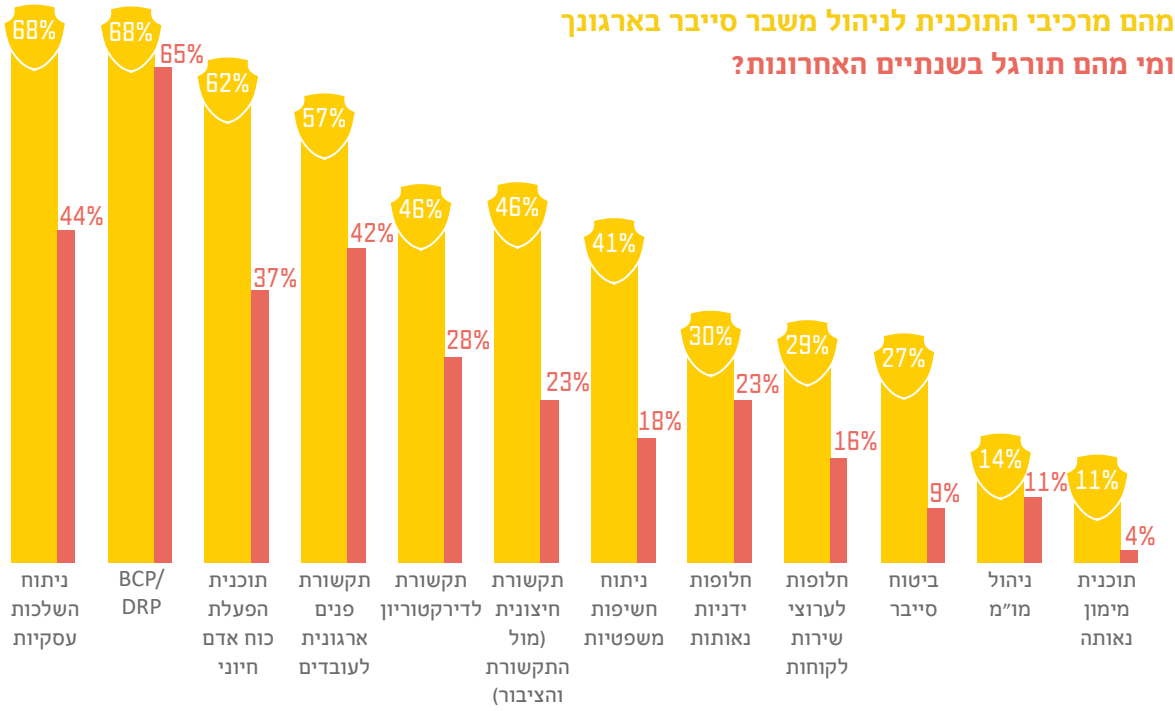
תגובתה של החברה ומהלכי פתרון הבעיות הראשוניים שניסתה לבצע, באורח מבולבל ועמום, עשויים להעיד שלא הייתה לה תכנית חירום מתורגלת וברורה להתמודדות עם אירוע סייבר שכזה. יומיים לאחר התקיפה התראיינה המנכ"לית לרשת בי.בי.סי. היא נראתה מבולבלת וחסרת אונים, לא ידעה לספק פרטים על זהות הגורם שתקף את החברה, על אומדן הנזק, על יעדי הפגיעה ועל הסיבה לתקיפה. כמו כן, המנכ"לית סיפקה בריאיון מספר אמירות תמוהות, כמו ההבחנה שלפיה "הימים שבהם מידע נגנב כדי למכור אותו ברשת האפלה כמעט אינם, זה כבר לא כל כך רווחי". על פי הערכות, החברה איבדה מעל 250,000 לקוחות, והנזק מהתקיפה הוערך ב-60 מיליון ליש"ט, וכלל היבטים כגון הוצאות לצוותי התגובה לאירוע, עלויות IT, יועצים חיצוניים, פורנזיקה, שיקום המוניטין, אובדן מכירות, עלויות שדרוגים חינם וכו' .

לאור ממצאי הבדיקה של ה-ICO (הרגולטור הבריטי בתחום התקשורת), מנכ"לית החברה, הגברת דידו הרדינג, פוטרה 18 חודשים לאחר האירוע ובזיקה ישירה אליו.

לעומת זאת, באוקטובר האחרון נתקפה חברת תשתית ה-DNS האמריקאית DYN במתקפת מניעת שירות, יש שיאמרו הגדולה בהיסטוריה, על ידי עשרות אלפי רכיבי IoT. אחת הסיבות המרכזיות שבגללן הם הצליחו לטפל באירוע בתוך שעות ספורות היה תרגול, כפי שהעידו על עצמם: "אנחנו מתאמנים ומתכוננים לתרחישים כאלה על בסיס קבוע. אנחנו מתרגלים תסריטים מתגלגלים (playbooks) ועובדים עם שותפים כדי להתמודד עם תרחישים כאלה".

בהמשך לכך, עולה מהסקר כי הנושאים הבאים לא מתורגלים באופן מספק: ניהול משא ומתן עם תוקף, ערוצי תקשורת חלופיים עם לקוחות וניתוח חשיפות משפטיות. אי תרגול נושאים אלה מהווה חשיפה לארגון ופוגע ביכולת שלו להגיב בצורה נאותה בזמן אירוע, שכן כל אלה הן יכולות שללא תרגול קשה מאוד ליישם אותם בזמן אירוע.

מהם מרכיבי התוכנית לניהול משבר סייבר בארגונך ומי מהם תורגל בשנתיים האחרונות?



סיכום

שנם ארגונים שיבחרו להמשיך לעצום עיניים ולקוות לטוב, אולם הנהלות וארגונים שמעדיפים לנהוג באחריות כלפי הלקוחות, העובדים ובעלי העניין האחרים, ייערכו לא רק בגזרת ההגנה אלא גם ייערכו לניהול אירוע סייבר, בין היתר על ידי הגדרת נוהלי תגובה, מינוי צוות לניהול אירוע סייבר ותרגול תרחישים רלוונטיים.