פיתוח יכולות ארגוניות לניהול משברי סייבר

גבי סיבוני והדס קליין

מספר גדל והולך של אירועים בתחום ביטחון הסייבר ומורכבותם הביא ארגונים רבים לפתח נהלים ויכולות לטיפול בתקריות סייבר. אלה מתבשאים ביכולות לתגובה מיידית לאירועים, ביכולות טכנולוגיות ובהקמת צוותים לתחזוקת מערכות המידע בארגון. יכולות אלו עשויות להיות בלתי מספקות, שכן לעיתים הן חסרות התייחסות להיבטים ניהוליים, לכישורים ולכלים הנדרשים מהצוות הטכנולוגי לניהול המשברים במהלך ההתמודדות עם תקרית סייבר. מצב זה עלול לגרום להידרדרות מהירה וחסרת שליטה של המצב ולהפוך למשבר חמור בעל היבטים פיננסיים, משפטיים ותדמיתיים, המשפיע על נכסי הארגון כולו. מאמר זה יבחן את הדרכים לפיתוח יכולות ארגוניות שיאפשרו להתמודד ביעילות עם משברים במערכות המידע, התקשוב והסייבר.

מילות מפתח: סייבר, משבר סייבר, ביטחון סייבר, התאוששות, ניהול משברים, המשכיות עסקית

מבוא

במאי 2017 התרחש משבר חמור בחברת התעופה British Airways. לדברי החברה, כֶּשל בחוות שרתים, שנגרם מנחשול חשמלי שנבע מפעולת כיבוי והדלקה של המערכת, השבית את יכולת החברה להפעיל את טיסותיה במשך שעות ארוכות. כתוצאה מכך התבטלו טיסות רבות ולמעלה מ־75,000 נוסעים לא יכלו להגיע ליעדיהם. הנזק לחברה התעצם כתוצאה מהקושי של הגורמים המקצועיים להבין את מהות התקלה ולטפל בה באופן שימזער את הנזק הן לחברה והן לנוסעים.[1] כתוצאה מכך, הנזק לחברה בכסף ובמוניטין היה ועודנו עצום. אירוע זה היווה

ד"ר גבי סיבוני הוא ראש תוכנית ביטחון סייבר במכון למחקרי ביטחון לאומי. הדס קליין היא חוקרת בתוכנית ביטחון סייבר במכון למחקרי ביטחון לאומי.

1 Nicola Harley, "British Airways IT Crisis Mystery as Energy Suppliers Say there Was No Power Surge", *The Guardian*, May 31, 2017.

תזכורת עד כמה חיוני להקים ולתרגל מערך ניהול משברים בחברות הנשענות על תשתיות מחשוב לצורך פעולתן.

מרבית המנהלים מבינים כיום כי אירוע סייבר הינו בלתי נמנע. אין זה משנה עד כמה מקצועי יהיה צוות ההגנה של הארגון, סביר להניח כי במוקדם או במאוחר יימצא הארגון תחת מתקפת סייבר ויחווה ניסיונות פריצה או פגיעה בתפקוד מערכות המחשוב שלו. אשר על כן, חברות וארגונים משקיעים כיום רבות ביכולות הגנה פרו־אקטיביות שמטרתן היא לאתר מתקפות בשלבים המוקדמים ביותר, עוד בטרם הצליח אירוע הסייבר להתממש ולגרום נזק של ממש. במסגרת זו משקיעים ארגונים גם בגישות ובכלים חדשים, כגון: מודיעין סייבר, ניטור רציף של רשתות וכלים לזיהוי התנהגות אנומלית. יחד עם זאת, ועל אף אמצעי ההגנה, על ארגונים להמשיך לוודא שיש ביכולתם להתמודד עם משברים שמקורם באירועי סייבר חמורים.

בשנים האחרונות התרחשו בקרב מגזרים שונים מספר משברי סייבר שהתפתחו לממדים משמעותיים, לעיתים עקב כשלים בניהולם. משברי סייבר מסוג זה עשויים לגרום לפגיעה באמון הלקוחות, בהכנסות החברה, במוניטין שלה ועוד. משברי סייבר מאיימים לעיתים גם על מנהלים באופן אישי ועשויים לגרום להם לאבד את תפקידם.

דוגמה לכשלים בניהול משבר סייבר בשל היערכות לא נאותה ניתן לראות במשבר אותו חוותה ספקית התקשורת הבריטית TalkTalk באוקטובר 2015. אופן ניהול המשבר שאיתו התמודדה החברה מעיד כי היא פעלה באופן מבולבל, עמום ולא עקבי, דבר המוביל למסקנה כי לא הייתה לה תוכנית ניהול משברים ברורה.[2] יומיים לאחר היוודע דבר התקיפה, החברה לא הצליחה לבודד את הנזק, לאמוד אותו ולזהות את התוקף וגם לא את הסיבה לתקיפה. על פי הערכות, הנזק לחברת TalkTalk כתוצאה ממשבר זה עמד על שישים מיליון ליש"ט וכלל הן נזקים ישירים והן נזקים עקיפים, שהתבטאו בפגיעה במוניטין, באיבוד לקוחות ועוד. כשנה וחצי לאחר האירוע, ולאור בדיקת הרגולטור הבריטי, פוטרה מנכ"לית החברה. מדוח הרגולטור עולה בבירור כי המנכ"לית הייתה אחראית לחוסר המוכנות של החברה להתמודד עם משבר סייבר.

להבדיל מהמקרה של חברת TalkTalk, חברת התשתיות האמריקאית DYN, שחוותה באוקטובר 2016 מתקפת מניעת שירות מהחמורות שנראו עד היום, הצליחה בתוך שעות ספורות להדוף את המתקפה ולמנוע את הסלמתה למצב משברי. עובדי החברה העידו כי הם מתאמנים ומתכוננים לתרחישים מסוג זה על

2 Lucas Fettes, "What Lessons Can All Organizations Learn from the TalkTalk Security Breach?", November 12, 2015, http://www.lucasfettes.co.uk/what-lessons-can-all-/organisations-learn-from-the-talktalk-security-breach.

בסיס קבוע, וכי התרגול אינו ממוקד אך ורק בהיבטים טכנולוגיים, אלה כולל גם תהליכי הערכת מצב, קבלת החלטות תחת לחץ ותקשורת עם הדרג הניהולי.[3]

בניית יכולת ארגונית להתמודדות עם משבר מחשוב וסייבר ראוי שתהיה רכיב חיוני בבנייה הכוללת של יכולות ההגנה וההמשכיות העסקית של כל ארגון. מאמר זה מנתח את הרקע התיאורטי של ניהול משברים ומציע לבחון פיתוח של ארבעה רכיבי יסוד שיאפשרו לארגון להתמודד בהצלחה עם משברי מחשוב וסייבר: פיתוח תפיסה ארגונית להתמודדות עם משבר מחשוב וסייבר; פיתוח כוח האדם וארגונו במסגרת צוות ניהול משברים; רכישה או פיתוח של כלים טכנולוגיים ותהליכים ארגוניים שיוכלו לסייע למימוש התפיסה הארגונית; בניית תוכנית הטמעה, הכוללת אימונים, תרגילים וסימולציות.

קלאוזביץ כתב בשעתו כי "המלחמה היא ממלכת אי־הוודאות".[4] כלל זה נכון גם למשברים במרחב הסייבר, שכן אי־הבהירות, הערפל השורר במהלכם והקושי לגבש תמונת מצב מקשים על קבלת החלטות ועל ביצוע הפעולות שיביאו לפתרון המשבר ולהתאוששות מהירה ממנו. פיתוח יכולות כאלו יביא בהכרח להתמודדות טובה יותר עם המשבר, לניהולו בצורה טובה יותר, ומכאן גם לתוצאות טובות יותר עבור הארגון.

רקע תיאורטי – אסטרטגיה של ניהול משברים

בתחום הסייבר, כמו בתחומים אחרים, יש חוסר אחידות באשר למושג "משבר" ולאופן השימוש בו. לעיתים קרובות נעשה שימוש נרחב מדי במושג זה. ככלל, לא כל אירועי הסייבר בארגון מובילים בהכרח למשבר תפקודי המחייב התייחסות מיוחדת. רוב אירועי הסייבר מטופלים באמצעות תהליכי שגרה, כגון טיפול בהדבקה של נוזקות, התמודדות עם מתקפות מניעת שירות קלות וכדומה. בדרך כלל, אירועים אלה אינם פוגעים בארגון בטווח הבינוני והארוך, וההתמודדות איתם הינה לחם חוקם של צוותי ביטחון הסייבר או אבטחת המידע. אולם, יש ואירועי סייבר חמורים יגרמו לפגיעה מתמשכת ביכולת הארגון לתפקד ולספק שירות ללקוחותיו. במצב כזה מדובר באירוע משברי המחייב התמודדות מיוחדת.

אולגה קוליקובה ועמיתיה[5] מנתחים את משמעות חשיפתו של משבר סייבר בארגון וטוענים שלחשיפה כזאת יש ארבעה היבטים משמעותיים: הראשון נוגע

---

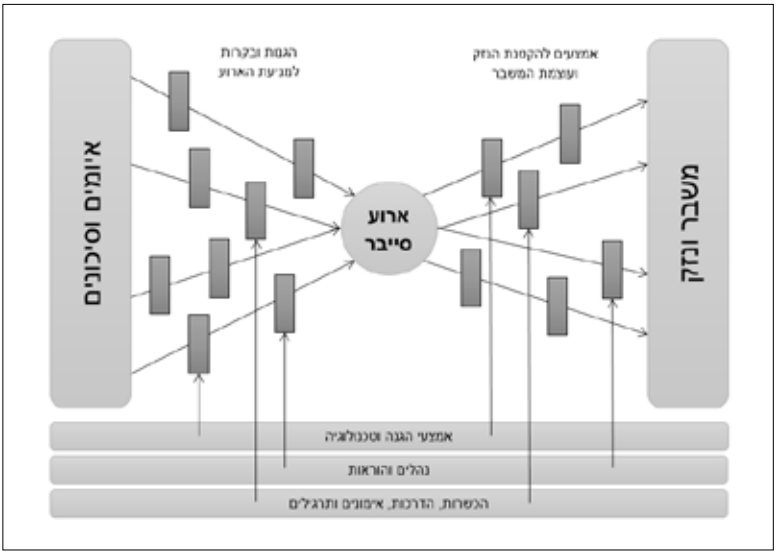
3 Christopher Roach, "Lessons Learned from the Dyn Attack", *CFO.com*, February 9, 2017, http://ww2.cfo.com/cyber-security-technology/2017/02/lessons-learned-dyn-attack.

4 רוג'ר אשלי לאונרד, **על המלחמה – מדריך קצר לקלאוזביץ**, משרד הביטחון־ההוצאה לאור, תל אביב, 1977, עמ' 79.

5 Olga Kulikova, Ronald Heil, Jan van den Berg, Wolter Pieters, "Cyber Crisis Management: A Decision-Support Framework for Disclosing Security Incident

לשיפור ההגנה ושיפור היכולת לבנות תמונת מצב; השני נוגע לעובדה שהחשיפה תאפשר לשפר את העמידה ברגולציות ובתקנים; השלישי נוגע לאפשרות שהחשיפה עשויה לפגוע בחוסן הכספי של הארגון; הרביעי נוגע למוניטין של הארגון העשויים להיפגע כתוצאה מהמשבר, דבר שמצידו עלול להקרין על התוצאות העסקיות של אותו ארגון.

אחד המודלים המנתחים את תהליך ההתמודדות עם אירוע משברי הינו מודל "עניבת הפרפר" (Bow-tie) שפותח כבר בשנת 1979.[6] מודל זה מציב את האירוע במרכז ומאפיין את ההגנות והבקרות שנועדו למנוע אותו, וכן את האמצעים שיש לנקוט להקטנת הנזק כאשר האירוע התרחש. התרשים שלהלן ממחיש את המודל בהקשר לאירוע סייבר:



תהליך ההתמודדות עם אירוע משברי מחייב בניית יכולות לגיבוש תמונת מצב מתמשכת במהלך המשבר. זהו תהליך המחייב מעקב קבוע אחר הפרמטרים המתפתחים של המשבר. "תמונת מצב" הינה ביטוי בו משתמשים בעת ניהול משבר בכדי לתאר את ההערכה הטובה ביותר למתרחש ברגע נתון, מה עשויות להיות ההשפעות של התרחשות זו, מידת חוסר הוודאות בהערכה, מידת יכולת ההכלה

Information", *IEEE, Computer Society, 2012 International Conference on Cyber Security*, pp. 103-112.

6 Steve Lewis and Kris Smith, "Lessons Learned from Real World Application of the Bow-tie Method, Prepared for Presentation at American Institute of Chemical Engineers", *6th Global Congress on Process Safety*, San Antonio, Texas, March 22-24, 2010.

של המשבר, כיצד הוא עשוי להתפתח ולהחמיר ומה עשוי להתרחש בהמשך. עוד מתארת תמונת המצב את ההגנות הפעילות והזמינות לארגון אל מול האיומים. תמונת המצב משמשת כבסיס להערכת המצב לצורך קבלת החלטות אופרטיביות ותעדוף האירועים והטיפול בהם, וזאת בהתחשב ברמת הסיכון ובפוטנציאל הנזק הגלום בהם.

החשיבות של תהליך בנייתה של תמונת המצב מתוארת במאמר של עלי רשידי ועמיתיו.[7] המאמר מנתח תהליך זה במהלך אירוע סייבר כמרכיב קריטי ביכולת לקבל החלטות מושכלות. מחברי המאמר מציעים מודל להיתוך מידע כדי לאפשר תהליך רציף של התעדכנות, תוך התבססות על מערכות מומחה.

מאמרם של בארפורד ועמיתיו מנתח את השלבים של תהליך בנייתה של תמונת המצב.[8] בשלב הראשון נדרשת הבנה של מה שקורה באותו רגע. שלב זה מותנע לאחר שמתקיים תהליך ראשוני של מיון ההתרעות שמתקבלות וניתוח הנתונים הקיימים. התהליך נמשך במטרה להבין את משמעות האירוע ואת מידת השפעתו על התהליכים הקריטיים בארגון. בשלב הבא מציעים הכותבים לגבש הבנה באשר לתהליך התפתחותו של האירוע, ולבסוף לגבש הבנה באשר לשאלה כיצד הוא התרחש. כל אלה הינם שלבים מקדימים לתהליך הערכת המצב, שמטרתו היא לקבל החלטות לפעולה לצורך הכלת האירוע ומזעור הנזק שהוא גורם.

ממד הזמן יוצר מורכבות נוספת. פעמים רבות קיים קושי להגדיר את המעבר מאירוע סייבר בעל עצימות נמוכה, שכדי להתמודד איתו מופעלים בשגרה אנשי הצוות הטכנולוגי והאירוע כולו נשאר בגבולות אלה, לבין אירוע סייבר בעל עצימות גבוהה, שמתפתח למשבר בעל השלכות משמעותיות לארגון כולו ומצריך מעורבות של יכולות נוספות. ניתן לתאר את נקודת המעבר מאירוע סייבר שגרתי לאירוע סייבר משברי באופן הבא: בשלב ראשון נוצר פער סמוי בין אופן התפקוד של מערכות המחשוב ובין המצב הרצוי, כפי שהוא מוגדר ברמות השירות הארגוניות. הטיפול בשלב זה נעשה על ידי גורמי השגרה. במידה והאירוע מידרדר, הפער גדל, צובר תאוצה ועלול להתרחב לתחומים נוספים, נדרש טיפול רחב ועמוק יותר.

הוראה 361 של בנק ישראל מגדירה מספר שלבים בהתמודדות עם אירוע סייבר:[9] שלב הזיהוי (Detection), במהלכו מתבצע בירור ראשוני בדבר קיומו של אירוע סייבר; שלב הניתוח (Analysis), הנוגע לבירור מקיף ומעמיק ככול האפשר

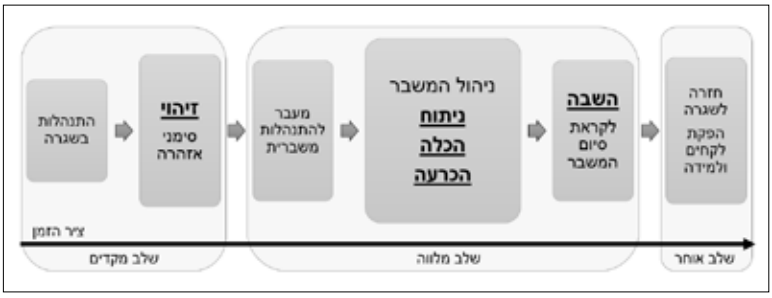
7 Ali J. Rashidi, Kourosh D. Ahmadi, Mostafa Heidarpour, "Cyber Situational Awareness Using Intelligent Information Fusion Engine (IIFE)", *Cumhuriyet University Faculty of Science, Science Journal (CSJ)*, Vol. 36, no. 3 (Special Issue), 2015.

8 P. Barford et al., "Cyber SA: Situational Awareness for Cyber Defense", *Cyber Situational Awareness* (Springer US, 2010).

9 המפקח על הבנקים, הוראה 361, ניהול בנקאי תקין [1] (3/15), **ניהול הגנת הסייבר**, מארס 2015.

לגבי אירוע הסייבר, וזאת לצורך קבלת החלטות בדבר כיווני פעולה אפשריים לבלימת התקיפה; שלב ההכלה (Containment), שנועד להשיג שליטה ראשונית באירוע לצורך הכלתו ועצירת החמרתו, עד להשלמת ההכלה; שלב ההכרעה (Eradication), שמטרתו נטרול האירוע כדי למזער ככול הניתן את הנזק שגרם; שלב ההשבה (Recovery), במהלכו חוזר הארגון לתקינות פעולה מלאה.

ניתן לאפיין את היכולות הנדרשות להתמודדות עם המשבר על פי שלביו הכרונולוגיים: הראשון הינו השלב המקדים בשגרה. בשלב זה על הארגון לקיים פעולות להפחתת ההיתכנות להתפתחות משבר ולהגברת המוכנות וההיערכות לניהולו. בספרו של סיימון בות', **אסטרטגיה של ניהול משברים**, הוא מונה מספר פרמטרים המקרינים על יכולת הארגון להתמודד עם משבר, אותם יש לפתח בשלבים המקדימים. הפרמטר הראשון הוא תכנון. בשלב המקדים נדרש הארגון להשקיע משאבים בתכנון ההתמודדות עם משבר.[10] משהוטל הארגון לתוך מציאות משברית, עוברים לשלב השני – השלב המלווה הכולל את ניהול המשבר בפועל – שם נדרש מגוון של יכולות שיסייעו לארגון בהתמודדות עם המשבר ובמזעור הנזק. השלב השלישי הוא שלב ההתאוששות לאחר האירוע, הכולל את תחקיר האירוע והפקת לקחים ממנו. הצגת שלבים אלה על ציר הזמן מומחשת בתרשים שלהלן:



פיתוח תפיסה לניהול משברים

אבן הדרך הראשונה הינה פיתוח תפיסה ארגונית לניהול משברים. תפיסה זו צריכה לכלול מספר מרכיבי יסוד: הראשון שבהם נוגע לקביעת מדדים לזמן השבתה נסבל ולרמות התפקוד הנדרשות לכול מערכת מחשוב בארגון. תהליך זה מחייב הסתמכות על ניתוח מערכות המחשוב והקריטיות שלהן לתפקודו הכולל של הארגון. ניתוח זה נקרא Business Impact Analysis (BIA), והינו רכיב בבניית תוכנית ההמשכיות העסקית. באמצעות כלי זה ניתן לנתח ולקבוע את ממדי

10 Simon A. Booth, *Crisis Management Strategy: Competition and Change in Modern Enterprises* (Routledge, Taylor and Francis Group, 1993), p. 13.

התפקוד של כל מערכת ואת הזמן הנדרש לה לחזרה לפעולה תקינה. קביעה כזאת מקרינה באופן מיידי על הקצאת המשאבים לצורך ניהול המשבר בארגון, שהרי לא דין ארגון שיכול להרשות לעצמו ניתוק מלקוחותיו למספר שעות, כדין בנק שהפסקת השירות המקוון שלו עלולה להסב נזק כספי ולפגוע במוניטין, או כדין חברת תעופה הנאלצת לבטל טיסות.

פיתוח התפיסה נדרש גם לצורך הגדרת מצבי משבר וליצירת שפה משותפת וכללים ברורים לניהולו. לקביעת מצבי המשבר וחומרתם יש השלכה מיידית על המשאבים אותם נדרש הארגון להקצות לצורך ניהול המשבר. משאבים אלה אמורים להתייחס להיקפו של צוות ניהול המשברים, למיומנויות הנדרשות ממנו, לאמצעים הטכנולוגיים והאחרים שיש להקצות לצורך הפעלתו, ולבסוף להיקף ההכשרות והאימונים של צוות זה. לאחר הגדרת מצבי המשבר נדרשת התפיסה לקבוע את תהליכי העבודה בארגון בשגרה, טרם המשבר, וכן במהלכו, ולבסוף לקבוע את תהליכי התחקור והלמידה בעקבותיו. התפיסה גם נדרשת לקבוע את אחריותם של בעלי התפקידים בארגון במצבי משבר.

פיתוח התפיסה והמורכבות של משברי סייבר ושל משברים ארגוניים בכלל מצריכים שיתוף גורמים רבים בארגון, בנוסף לצוותים המספקים מענה טכנולוגי לשירותי המחשוב ולאמצעי התקשורת. שיתוף זה דורש תיאום וניהול של מספר דיסציפלינות, ובהן ניהול ההשלכות המשפטיות הקשורות בתפעול והשגחה על מאגרי מידע, ניהול חבויות רגולטוריות הנכנסות לתוקף מרגע הכרזת המשבר, ניהול הפגיעה במוניטין, שיתוף הממונה על הסיכונים, עירוב גורמים הממונים על הגנת הסייבר בקרב רשויות האכיפה ועוד. לפיכך, חשוב לקבוע ועדת ניהול משברים ארגונית כחלק מההיערכות לניהול משבר סייבר, ולכלול בה את הצוות הניהולי הבכיר בארגון, כגון המנכ"ל, מנהל הכספים, היועץ המשפטי וגורם יחסי ציבור.

היתרונות הבולטים של שילוב מנהלים בכירים בוועדה לניהול משברי סייבר הם היכולת והסמכות לפעול בשני מישורים משלימים: בשגרה תפעל הוועדה לבחון היבטים רגולטוריים ומשפטיים בתרחישי משבר שונים ולהגדיר היבטים פיננסיים הקשורים בניהול משברים, תתקף את תוכניות ההסלמה במעלה מדרג הניהול ואת תוכניות המגירה לניהול ערוצי התקשורת והמדיה השונים בעת התרחשות משבר; בעת משבר תסייע הוועדה לאזן בין המתרחש בתוך הארגון ומחוץ לו ולשמור על המוניטין שלו, וכן תפעל להקטנת ההתחייבויות המשפטיות המתעוררות במהלך אותו משבר. כל זאת, תוך שמירה על אובייקטיביות ועל תהליכי תעדוף.

פיתוח כוח אדם וארגונו בצוות ניהול משברים

אחד היתרונות בהכשרת צוות פנים ארגוני לטיפול במשברים הינו היכולת של צוות כזה לנתח את מכלול האפשרויות ודרכי הפעולה באופן מיטבי. סביר להניח

כי אף גורם חיצוני, עתיר ניסיון ככול שיהיה, לא מכיר את הארגון כמו הצוותים המקצועיים, מנהלי התהליכים העסקיים והנהלת הארגון. זאת ועוד, חברי הצוות הפנים ארגוני הם, על פי רוב, בעלי סמכות מקצועית וזוכים להכרה ככאלה, דבר האמור להקל עליהם בעת ניהול האירוע.

כדי לנצל את המשאבים הפנימיים של הארגון ולממש את התפיסה הארגונית, יש צורך בהכשרת כוח אדם. תהליך בחירתם של בעלי התפקידים השונים מחייב הגדרה ברורה של מכלול התפקידים, של אחריות הצוות לניהול משברים ושל הממשקים שלו עם בעלי עניין בארגון ומחוצה לו. כמו כן, יש להגדיר את הכישורים הנדרשים מבעלי מקצוע אלה.

הדרישות מכול בעל תפקיד במהלך משבר צריכות לכלול קביעה של תחומי האחריות, ניתוח מערכת הכישורים הנדרשת והגדרה של הידע והניסיון הדרושים. בשלב הבא יש להגדיר את המיומנויות והכישורים הניהוליים הנדרשים מחבר הצוות כדי שיוכל למלא את תפקידו. הגדרה זאת צריכה לענות על השאלה "איזה מיומנויות וכישורים נדרשים כדי לנהל את המשבר באופן יעיל, ומה צריך חבר הצוות כדי לפעול ביעילות?". בשלב השלישי יש להגדיר את הידע והניסיון שצריכים להיות מצויים אצל כל חבר בצוות ניהול המשברים. כל אחד מאלה צריך להכיר היטב את הסביבה העסקית ולא רק את הסביבה הטכנולוגית, ולכן חייב להיות בעל היכרות עם הפעילות העסקית של הארגון, לפחות ברמה של הבנה בסיסית. הבנה כזאת תספק לו את היכולת לתעדף את אופן הטיפול במשבר על בסיס הבנת הקריטיות של התהליכים העסקיים שנפגעו.

הצוות הטכנולוגי של הארגון נדרש להתמודד עם מגוון אתגרים בעת משבר סייבר, בהם: גיבוש תמונת מצב, בדרך כלל על בסיס מידע חלקי, וגיבוש המענה המיטבי במטרה להתאושש במהירות ולשוב לתפקוד סביר. במקרים בהם המשבר מלווה בלחץ ציבורי נרחב, נדרשים מנהלי הארגון לתת תשובות לציבור הלקוחות ולבעלי עניין אחרים, דבר שמגדיל עוד יותר את תחושת הלחץ בה נתונים הגורמים המקצועיים.

הצוות הטכני לניהול משברים הוא הגוף הממונה על ניהול המשבר בארגון בהיבטים הטכנולוגיים והוא זה שמנחה את הגורמים המקצועיים כיצד לטפל בו באופן שיצמצם את הנזק והפגיעה במוניטין של הארגון. השאיפה היא שהצוות הטכני גם יצליח למנף את המשבר לטובת הארגון. תפקידיו של צוות זה כוללים גם היבטים של הערכה ראשונית של הנזק, תקשור המצב הקיים והשלכותיו העסקיות, גיבוש תוכנית פעולה למנהלי התהליכים העסקיים ולהנהלה, הכרזה על מצב חירום וניהול האירוע. אלו הן משימות מורכבות שאינן מסתכמות בהיבטים טכנולוגיים ובהבנה והיכרות של מערכות המחשוב והתקשורת הקיימות בארגון, אלא מצריכות גם הבנה עסקית, משפטית ותקשורתית רחבה.

צוות ניהול המשברים נמצא בעת משבר תחת לחץ רב שעשוי להקשות על תפקודו. תחושת הלחץ גוברת ככול שגדֵל הפער בין האמצעים והכישורים הדרושים לצורך התמודדות עם המשבר ובין היכולת והמשאבים העומדים בפועל לרשות הצוות. ניתן לאפיין שני סוגים של כישורים הנדרשים לצוות: כישורים מקצועיים/טכנולוגיים שעניינם התמצאות עמוקה במערכות הטכנולוגיות והניהוליות של הארגון; כישורים רכים שעניינם פיתוח יכולות אישיות וקבוצתיות המסייעות בתהליך ניהול המשבר.

פיתוח הכישורים המקצועיים/טכנולוגיים הינו תהליך המחייב הכשרה והתמקצעות במגוון המערכות הטכנולוגיות של הארגון, ובכלל זה מערך התשתיות והתקשורת, שרתי הנתונים ויישומי הקצה של הארגון. זאת, לצד הבנה עמוקה במערך הניהולי, ובכלל זה בתהליכי קבלת ההחלטות, במערך הסמכויות ובמקורות הידע בארגון, ובנוסף לכך הבנה של כלל המערכות והתהליכים הקריטיים בארגון ברמה שתאפשר ניתוח אירוע ומיפוי הגורמים הרלוונטיים לטיפול בו. כדי לשפר את ההבנה העסקית/ארגונית של צוות ניהול המשברים, מומלץ לקיים מפגשים קצרים עם מנהלי התהליכים העסקיים הקריטיים בארגון ולחשוף את צוות ניהול המשברים למורכבות, לחשיבות ולאתגרים הקשורים באותם תהליכים.

ראש צוות ניהול המשברים צריך להימנות על הדרג הניהולי וחשוב שיהיה בעל היכרות עמוקה עם ההיבטים הטכנולוגיים והשלכותיהם על התהליכים העסקיים. הייס ואומודיי קובעים כי מה שנחוץ לראש צוות ניהול המשברים הוא שילוב של תכונות אישיות ותכונות בין־אישיות. מדובר בתכונות של סובלנות ללחץ, במוּדעות עצמית ובמודעות כלפי כל אחד מחברי הצוות, וכן במיומנויות תקשורת טובות.[11]

צוות ניהול המשברים צריך לכלול חבר צוות שיהיה ממונה על היבטים הקשורים בתיאום המשבר בין היחידות העסקיות. על חבר צוות זה להיות בעל היכרות טובה עם מבנה הארגון ועם היבטים מינהליים הקשורים בתפקודו. הצוות אמור לכלול גם אנשי טכנולוגיה בעלי ידע מצטבר בתחומי התשתיות, התקשורת, השרתים, היישומים ובסיסי הנתונים. במקרים בהם המשבר חולש על מספר אתרים של הארגון, יש חשיבות להצבת נציגים של צוות ניהול המשברים בכול אתר, והתיאום העליון צריך להתבצע באופן מרוכז.

המאפיינים האישיים של אנשי הצוות לניהול משברים צריכים לכלול, כאמור, גם כישורים רכים, ובהם מיומנויות ותכונות כמו תקשורת בין־אישית, יכולת הקשבה, אינטליגנציה רגשית, כושר שכנוע, יצירתיות, קפדנות, יכולת לפתרון בעיות, יכולת

11 P. A. Hays & M. M. Omodei, "Managing Emergencies: Key Competencies for Incident Management Teams", *The Australian and New Zealand Journal of Organizational Psychology*, February 2012.

לעבודה בצוות, יכולת לקבל החלטות תחת לחץ ועוד. תכונות אלו ניתנות לפיתוח ולשיפור, כשהמטרה היא להביאן לידי ביטוי במסגרת ניהול המשבר.

שכנולוגיה

כלים רבים מסייעים בתהליך ניהול האירועים. במסגרת התפיסה הארגונית יש להחליט האם לעשות שימוש בכלי מדף או לייצר כלי ייעודי, הכול בהתאם לצרכים הייחודיים של הארגון.

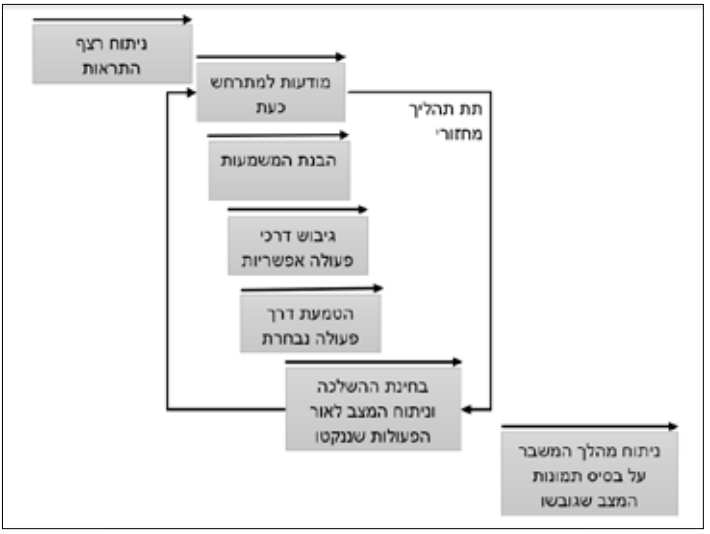
לכלים הטכנולוגיים יש חשיבות רבה בתמיכה בתהליך ניהול המשברים בארגון. כלים אלה נדרשים לתת מענה למגוון השלבים בתהליך, בכללם תהליכי גיבוש תמונת המצב וביצוע הערכת המצב, ולספק מערכת תומכת לניהול משברים, כולל יכולת שימור ואחזור מידע ממאגרי ידע מאירועים קודמים בארגון עצמו ובארגונים אחרים, וכן יכולות תיעוד לצורכי למידה. המערכת לניהול משברים מאפשרת מעקב ממוכן אחר הנהלים והתהליכים השונים ומדגישה את סדרי העדיפויות בניהול האירוע באמצעות תרחישים המוזנים מראש ומתבססים על תהליכים עסקיים קריטיים. היא גם מעצימה את התקשורת הפנים־צוותית והפנים־ארגונית.

ככלל, הכלי לניהול המשבר נועד לתת מענה למספר צורכי יסוד:

- ליצור יומן מבצעי שיהיה מאורגן באופן טבלאי ויפרט את מהלך ההתרחשויות והאירועים. שימוש ביומן מבצעי מאפשר לתעד את האירוע מהרגע הראשון ולשקף את המתרחש במהלכו. מטרתו היא לאפשר גיבושה של תמונת מצב, לתמוך בתהליכי קבלת החלטות ולתחקר את המשבר עם סיומו. יומן כזה צריך לכלול מועדי התרחשויות מדויקים, תיאור עדויות, עובדות והנחות עבודה.
- להוות פלטפורמה לתקשורת בין אנשי המפתח בארגון ובין בעלי העניין בעת האירוע. לעיתים נדירות בלבד נמצאים אנשי המפתח בו־זמנית בחדר ניהול המשבר, ועל כן נדרש לספק להם כלי שמאפשר תקשורת והבנת תמונת המצב מכול מקום ובכול עת.
- ליצור מרחב וירטואלי מרכזי אחד, בו יהיה מרוכז כל המידע על ההתרחשויות. יצירת מרחב כזה נועדה להבטיח שהצוותים הטכנולוגיים ומקבלי ההחלטות פועלים על בסיס אותן עובדות.
- לסייע בהבנת תמונת המצב בעזרת טווח הפרשנויות השונות של סיבה ותוצאה המאפיינות את עולם מערכות המידע, וזאת תוך התמודדות עם כמות ההתרחשויות ועם קצב האירועים המהיר.
- לסייע בהפחתת הלחץ לצורך קבלת החלטות אובייקטיביות והפעלה מובנית של תהליכי העברת הטיפול לדרג ניהולי גבוה יותר.

- לתמוך בתקשורת על פי מטריצת התקשורת וההסלמה הארגונית. מערכות לניהול משברים מאפשרות להזין מראש את מטריצת התקשורת ושולחות באופן אוטומטי עדכונים בעת התממשות התנאים שהוגדרו במערכת מראש.
- לסייע בהבנת משמעות האירועים, כך שפיסות המידע שנאספו ממקורות שונים יצורפו לכדי תמונה שלמה. זאת, תוך הערכת איכות המידע, הפרדה בין עיקר לטפל וארגון המידע בדרך שתאפשר לשלוף אותו בקלות בהמשך.
- לתמוך בתהליך הניסוח של דרכי פעולה אפשריות על בסיס הנתונים הידועים ותוך פירוש העובדות הרלוונטיות וניתוחן, וזאת כדי להבין כיצד המצב עשוי להתפתח.
- לבחון את ניתוח המצב ואת השלכותיו לאור הפעולות שננקטו. בשלב זה מתחיל מסלול חדש של גיבוש תמונת מצב והערכת מצב, המבוססות על השינויים שהתרחשו כתוצאה מהפעולות שננקטו ועל נתונים חדשים שהגיעו מבחוץ.

שימוש בכלים טכנולוגיים שיוכלו לסייע בתהליכים שתוארו לעיל יאפשר הגברה משמעותית של היעילות בעבודת הצוות לניהול המשברים. התרשים שלהלן מציג באופן סכמתי את התהליך אותו המערכות הטכנולוגיות נדרשות לתמוך:



משפחה נוספת של כלים טכנולוגיים נוגעת ללמידה מתוך אירועים קודמים בארגון ומחוצה לו. במהלך משבר אין מצפים מצוות ניהול המשברים לבצע ניתוחים שורשיים בכדי לזהות מדוע אירעה התקרית. ניתוח כזה צריך וחשוב שייעשה בתהליך התחקור אחרי האירוע, כחלק מהסקת המסקנות והלמידה הארגונית. ההתמקדות במהלך ניהול המשבר צריכה להיות בלימת אירוע הסייבר וסיכולו

ובהשבה מהירה של המערכות הארגוניות לתפקודן מלפני המשבר, תוך קביעת סדר עדיפויות. לפעמים נדרש פתרון זמני, או שימוש באמצעים שעוקפים את הבעיה, עד לפתרונה המלא.

כלי חשוב באבחון אירוע משברי הוא מסד הנתונים של האירועים והמשברים ההיסטוריים בארגון, אינדקס דומה המתאר את האירועים שהתרחשו במגזר העסקי אליו משתייך הארגון ברמת פירוט מרבית ככול הניתן, וכן אירועים שהתרחשו בסביבה הגיאופוליטית אליה משתייך אותו ארגון. למשל, ראוי שבנק ינהל רישום של אירועי סייבר חריפים שהתרחשו בבנקים אחרים ברחבי העולם. כלי כזה יאפשר לצוות ניהול המשברים בבנק לזהות בעיות או טעויות מוכרות שגרמו לאירועים דומים בעבר, ובכך לקבל מידע על דרכים לעקיפת הבעיות כשאלו זוהו. מדובר בכלי ממוכן ומובנה שצריך לכלול מנוע חכם לאחזור נתונים, כולל נתונים שנכתבו בפורמט של טקסט חופשי.

כלי ניהול המשברים גם נדרשים לתעד את המשבר ואת תהליכי העבודה במהלכו, וזאת כדי להזין את מערכת הלמידה הארגונית ולאפשר שימוש בה הן תוך כדי המשבר והן במשברים עתידיים. תיעוד המשבר חשוב שיכלול את השתלשלות העניינים, תיאור של ההתרעות שהתקבלו ואופן הדיווח עליהן, וכן ההחלטות שהתקבלו בכול שלב. לדבר זה יש חשיבות בכמה מישורים: למקרה ותרחיש דומה יתפתח בעתיד או למקרה בו, למרות הצעדים שננקטו ובכללם גיבוש תמונת המצב והערכת המצב, המשבר טרם הסתיים למעשה. בנוסף לכך, יש להקפיד על הכנת דוח מסכם שיופץ לבעלי העניין מבית, ובהם ההנהלה וגורמים נוספים בהתאם לעניין, וכן לבעלי עניין חיצוניים, על פי הנחיות הרגולציה המתאימות.

השמעה – הכשרה, אימונים ותרגילים

שיפור היכולות והשגת רמת מוכנות גבוהה מבוססים במידה רבה על אימונים, תרגילים והכשרות, כחלק מובנה בתהליך מימושה של התפיסה הארגונית. ניתן לאפיין מספר רכיבים בתהליך ההטמעה.

צוות ניהול המשברים כולל, בדרך כלל, עובדים בעלי הכשרה וידע עמוקים בתחום מערכות המחשוב ומרחב הסייבר הארגוני, שתפקידם בצוות בא בנוסף לתפקידם השגרתי. למרות זאת, כל מועמד לצוות ניהול המשברים צריך, טרם הפיכתו לחבר בו, לעבור הכשרת "שער כניסה", כלומר הכשרה בסיסית וראשונית. הכשרה זו צריכה לכלול את הכללים והעקרונות של הארגון לניהול משברים, את התוכניות והנהלים הארגוניים למצב כזה, הבנת הסביבה העסקית והיכרות עם כלים טכנולוגיים לניהול משברים. על ההכשרה גם לכלול היבטים של זיהוי, תיעוד, סיווג ותעדוף, אבחון (דיאגנוסטיקה) ראשוני של המשבר, חקירת התפתחותו, אמצעי התקשורת וההסלמה (העברת דרג הטיפול לרמה בכירה יותר), מקורות

המידע והאיסוף הקיימים בידי הארגון, ולבסוף אופן סגירת האירוע, תחקורו והפקת לקחים ממנו.

לצד ההכשרה הבסיסית, יש לקיים על דרך השגרה תרגילים, בכלל זה "תרגילי שולחן" (Tabletop Exercises) ואימונים לצוות בתנאים הקרובים ככול הניתן לתנאי אמת, וכן תרגילים רחבי היקף שישלבו גם את הרמה הניהולית בארגון. מטרתם של "תרגילי שולחן" היא לנתח תרחישי ייחוס רלוונטיים באופן שיאפשר למשתתפים בהם לבחון את התרחישים ללא הלחץ של סביבת העבודה. תרגילים כאלה מוסיפים באופן משמעותי לרמת הידע, מרחיבים את השפה המשותפת ומגבירים את רמת שיתוף הפעולה בין חברי צוות ניהול המשברים. במסגרת זו ניתן לעודד תהליכי חשיבה צוותיים, למקד את חברי הצוות בהתמודדות עם מגוון תרחישים ולשלוט על כיווני התפתחותם. זאת, תוך העמקת ממשקי התקשורת והאינטראקציה הפנימיים והחיצוניים עם בעלי עניין ושיפור ההבנה ההדדית באשר לסמכותם ואחריותם של חברי הצוות. תרגילים כאלה גם מאפשרים לתקף את המדיניות והנהלים של הארגון.[12] רצוי שהם יכללו הנחיה מקצועית[13] במטרה לסייע בהגברת רמת המוטיבציה של אנשי הצוות ובנכונותם להשתתף באירוע ולאפשר להם להתמודד איתו בהצלחה.[14] סט התרגילים מאפשר להוציא את צוות ניהול המשברים מחשיבה בתבניות כושלות, כגון חשיבה במושגים של הסתרה וטשטוש וניסיון לתת פתרון מיידי כדי לבצע "כיבוי שריפה".

לצד "תרגילי שולחן", יש לקיים אימונים ותרגילים רחבי היקף המדמים ככול האפשר את המציאות. ניתן לאפיין מספר עקרונות אותם יש לממש בתרגילים אלה:

- **אופי התרחישים** – גיבוש תרחישים הנוגעים לתקלות במערכות החיוניות של הארגון, תוך התבססות על ניתוח תוכנית ההמשכיות העסקית ועל ניתוח המערכות הקריטיות של הארגון (BIA). פעולה זו תבטיח התמודדות עם הליבה המבצעית של מרחב הסייבר הארגוני. מומלץ שתרחישי התרגילים ורמת מורכבותם ינוסחו באופן ספיראלי, כך שצוות ניהול המשברים ייחשף לתרחישים בעלי רמת מורכבות הולכת וגוברת.
- **סביבה טכנולוגית לתרגיל** – בניית סביבה טכנולוגית תרגילית שתאפשר דימוי קרוב ככול הניתן של המציאות. זאת, תוך מזעור השפעתו של התרגיל על התפקוד המבצעי של הארגון. הסביבה הטכנולוגית התרגילית צריכה לאפשר

12 Brent D. Ruben, "Simulations, Games and Experience-Based Learning", *Simulation & Gaming*, Vol. 30, 1999.

13 "Intrinsic Motivation, Extrinsic Rewards and Divergent Views of Reality", Book Review, *Educational Psychology Review*, Vol. 15, no. 3, September 2003.

14 A. J. Faria and W. J. Wellington, "A Survey of Simulation Game Users, Former Users and Never Users", *Simulation & Gaming*, June 2004.

תקשורת, הזרמת אירועים והקמת סביבת חיישנים למערכות המחשוב והתשתיות הטכנולוגיות.

- **בניית התרחיש** – התרגיל צריך להיבנות על בסיס האירועים המגיעים לצוות ניהול המשברים מהמערכות התפעוליות והמבצעיות וממפעיליהן. צוות ניהול המשברים יידרש לנסות לזהות את מקור התקלות מתוך בחינת האירועים והחיישנים הטכנולוגיים העומדים לרשותו (לדוגמה, עומס על משאבי מחשוב, תקלה בהעתקת נתונים ובקבצי לוג וכיוצא באלה). התרחיש נדרש לכלול את סיפור הרקע ואירועים המוזרמים במהלך האימון, שחלקם יהיו הזרמות "רעש" שאינן נוגעות ישירות לתקלות.
- **התאמות במהלך התרגיל** – צוות ניהול המשברים והמערכת הניהולית התומכת נדרשים לזהות את מקור הבעיה במערכות המחשוב ואת מהותו של אירוע הסייבר בו הם אמורים לטפל. לצורך זה יש להכין בנק אירועים שיוזרם בהתאם להתפתחות הטיפול בתרחיש, וזאת במטרה למצות את התרגיל ולאמן את כלל המעורבים באופן מיטבי.
- **בקרה וחניכה** – חיוני לקיים מערך בקרה צמוד לתרגילים. מערך זה יוכל להבחין במהלך התרגילים בחוזקות ובחולשות של כל חבר צוות ושל הצוות כמכלול, ובכך למקד את הלמידה ואת הפיתוח האישי והקבוצתי. במהלך התרגיל חשוב לכייל את היכולות הבסיסיות הקיימות ולהשתמש בנתונים שייאספו לצורך קביעת מדדי השיפור הנדרשים ולבחינת מידת ההצלחה של התרגילים הבאים. תוצאות התרגיל יאפשרו למקד את תוכנית ההשתלמויות והאימונים לחברי הצוות.

לצד אימון הצוות הטכנולוגי וכחלק מתהליכי האימון להתמודדות עם משבר, יש חשיבות לערוך אימון גם לרמה הניהולית בארגון. אימון כזה חשוב לצורך בניית שפה משותפת, להבנת האילוצים בכול הקשור לשיתוף בעלי עניין מחוץ לארגון במהלך משבר, וכן כדי לתת לצוות הטכנולוגי את השקט והמרחב הדרושים לטיפול במשבר ללא לחץ ניהולי. לחץ כזה לא רק שאינו תורם, אלא שברוב המקרים אף מפריע.

סיכום

ריבוי תקריות סייבר ומשברי סייבר הגביר מאוד את הצורך לפתח יכולות ארגוניות להתמודדות עם משברים כאלה. ניהול נכון של משבר סייבר יכול לצמצם נזקים ולהוביל את הארגון להתאוששות מהירה, ואילו כישלון בהתמודדות עם משבר כזה עלול להוביל לקריסת הארגון.

ניהול אירוע סייבר הינו משימה ארגונית הכוללת פונקציות רבות בארגון, החל מאנשי הסייבר ואבטחת המידע וכלה בחברי ההנהלה והדירקטוריון. לניהול האירוע יש השפעה שאינה נופלת מהשפעתן של היכולות הטכניות להתמודד איתו. יש

חשיבות מכרעת להכללת מדיניות לניהול משברי סייבר באסטרטגיית הסייבר הארגונית. על מדיניות זו לשקף את צורכי הארגון ויעדיו.

יכולת הארגון להתמודד עם משבר תלויה במידה רבה גם ביכולות האלתור והעמידה שלו בלחצים. נהוג ליחס יכולות כאלו לתרבות הניהול הישראלית, אולם אין בהן די במציאות המורכבת של משברי סייבר ובמצב הכאוטי שהם עלולים לגרום – מצבים שבהם נדרש צוות ניהול המשברים לתפקד. על כן, יש להתבסס על מתודולוגיות סדורות לניהול משברי סייבר ומחשוב ועל מערך מיומן שיוכן לצורך זה בעת שגרה. לאור זאת, מומלץ לנסח תוכנית מתאימה לפיתוח הכלים והמיומנויות בארגון, כפי שתואר במאמר זה, לרבות קביעת תוכנית סדורה לאימונים, סימולציות ותרגילים.