קורא יקר,

וירוסים, פרצות וספאם הולכים ומתרבים מיום ליום **באופן מבהיל.** מערכות המחשוב הופכות למורכבות וסבוכות. במקביל, הפס הרחב, הוירטואליזציה, BI - מציעים **הזדמנויות חדשות ומלהיבות** וגם תפקיד מנהלי המחשוב עובר טרנספורמציה **דרמטית ומבטיחה**. כך, לנוכח שטף חידושים וגלי תמורות, שרק מתעצמים ומואצים, קשה להתמקד במה שבאמת חשוב. **למי להאמין? על מי לסמוך?**

תחקירי PCאון מספקים בכל שבוע ריכוז של החדשות החשובות ביותר בעולם המחשוב והתקשורת, יחד עם תחקיר מקצועי שמתמקד בנושא מפתח מרכזי ומשמעותי. הם משרתים חלק גדול ממנהלי המחשוב המובילים של מדינת ישראל. חלקם מנויים לשירות קרוב לשש עשרה שנים כיוון ש:

- PCאון הוא מקור מידע **אמין ותכליתי.** הוא מתמקד רק **בנושאי המפתח** החשובים ביותר בעולם המחשוב והתקשורת, והוא **מדבר בשפתך המקצועית.**
- PCאון כולל את ריכוז **החדשות החשובות** ביותר וגם **מגמות, טיפים, ידע יישומי ושימושי** נוסף. הוא מאפשר בהשקעה של **פחות מ-10 דקות** בשבוע, להיות כל הזמן **עם יד על הדופק.**
- PCאון מביא תועלת בכך שהוא **רלוונטי לבעיות הנוכחיות שלך,** בנוסף לכך, הוא מסייע לך בהערכות מוקדמת בפני **סכנות ואיומים** למערך המחשוב **ו/או ניצול הזדמנויות עסקיות** חדשות.
- ניתן **להתרשם ממנו באופן אישי** באמצעות תחקיר הדוגמא המצורף או להסתמך על למעלה ממאה חוות דעת של מנהלי מחשוב מובילים (ראה - www.pcon.co.il/v5/103.asp).

PCאון נתפס כיום כ**מפתח מוכח להצלחה מהירה,** וככזה גם אתה תוכל ליהנות ממנו בקרוב. כמו ארגונים רבים תוכל להצטרף כמנוי ארגוני ותאפשר לכל העוסקים במחשוב בארגונך, ליהנות מכל היתרונות שלמעלה.

מחירי מנוי השנתי בגין 52 תחקירים:

מספר מנויים	המחיר בדולרים + מע"מ
1	516
5	1270
10	1970
20	3270
50	5970
100	7700
200 ויותר	9700

נכון, אפשר לנסות להתמודד לבד עם כל התמורות. להתעלם או לדגום מאמר אקראי ולקוות לטוב. **תחשוב על התוצאות.** מצד שני ניתן ללכת **בדרך סלולה ובטוחה** שבה הולכים המובילים במחשוב הישראלי, שגם ימשיכו להוביל בבטחה. כדי להצטרף אליהם, ללכת יחד איתם, אפשר לקרוא על תחקירי PCאון ולהצטרף באתר ב- www.pCon.co.il/promo טלפון 03-9667939, פקס 03-9660310 או מייל - sub@pcon.co.il

קובי שפיבק
העורך הראשי של PCאון

נ.ב. על כל תחקירי PCאון חלות כל ההגנות החוקיות של זכויות יוצרים. ביחד עם זה, אנו מתירים לשכפל ולהפיץ את תחקיר זה, **מבלי לשנותו, עד 31.12.2007 ורק יחד עם דף היתר זה!** למנהלים, עמיתים ואנשי מחשוב נוספים, שעשויים לדעתך למצוא בו עניין.

מה אתה מקבל? - מפתחות להצלחה

קורא יקר,

תיזכר ב"נפילה" האחרונה של מערכת בארגון, ב"פספוס" בבחירת טכנולוגיה, בפרוייקט שלא "סיפק את הסחורה". מדמיין? עכשיו קח לך פחות מחצי דקה ותחשוב על מי שקרא תחקיר דומה, לפני כשנה. באינטואיציה פנימית חזקה הוא הבין שמצא פיתרון אמיתי לצורך אמיתי - להיות ממוקד באיומים האמיתיים וההזדמנויות המבטיחות שרלוונטיים לארגון ולתפקיד שלו, למציאות שבה הוא חי. שוב ושוב הוא נוכח מאז, שהוא מתבסס על מקור מידע שמדבר אליו בשפתו, מקור תכליתי ואמין.

כאשר חבר קרוב מתקשר ושואל לחוות דעתו על תחקירי PCאון. "מה הם נותנים לך באופן מעשי?" באופן טבעי הוא נזכר ומספר על כמה מהדוגמאות הבאות:

- **בתחקיר - ה-IT מאיץ חדשנות** - הוא גילה את הטרנספורמציה שעוברת היום כגל סוחף בעולם העסקי. ה-IT הופך מכלי שתומך בעסקים, למנוע שמאיץ חדשנות ופותח הזדמנויות חדשות. התועלת עבורו הייתה דרך הסתכלות חדשה על היבטי ה-IT, כזאת שפתחה בפניו דלת לקידום מהיר...

- **בתחקיר - חוסכים חשמל** - הוא מצא נתונים לפיהם, עלויות החשמל של דטה סנטר בשנה יכולות להיות יקרות יותר מכל עלויות החומרה שבו. הוא גם קרא כיצד השינוי בצריכת החשמל בניידים לוקחת אותנו לעידן חדש. התועלת שהפיק מהתייחסות ויישום הייתה - הרבה כסף לארגון. איך זה נשמע?

- **בתחקיר - כללי אצבע למנמ"ר** - הוא מצא נתונים, מספרים, כללי אצבע ומקורות שחיוני לכל מנהל שעוסק במחשוב להיות מצויד בהם. התועלת שהפיק הייתה קבלת החלטות מהירות יותר, מבוססות ומוצלחות יותר. התוצאות נראות בשטח. מכיר אנשים כאלה?

- **בתחקיר - וירטואליזציה בשרתים** - הוא הבין את המשמעויות המעשיות של מגמה מרכזית שסוחפות כיום את עולם המחשוב, כאשר הוא גילה **איך** וירטואליזציה יכולה להעניק יותר גמישות, חיסכון עצום, שרידות, עבודה קלה ועוד יתרונות נוספים. פתאום הכול התחבר. אתה רואה זאת?

- **בתחקיר - Rootkit - חפרפרת במחשב** - הוא קרא כי ברשת הארגונית של כל ארגון חמישי באוסטרליה (וכנראה כך גם בארץ), חבויה כיום תוכנה נסתרת, שיכולה לפתוח דלתות לתוכנות מזיקות. בדרך כלל, לא ניתן לגלות אותה! גניבת מידע, שיבוש נתונים, האזנות, ציטוטים, חדירות, נזקים. חלק מהאיומים יכולים להביא לקריסה. הוא עשה את כל שניתן לטפל בכך וישן טוב בלילה. ואתה?

הוא גם לא היחידי שחושב כך. מאה המלצות נוספות עם מסר חד וברור מדברות בעד עצמן. אחרי הכול, עם הישגים שמוכחים בשטח, קשה להתווכח...

לכן אנו ממליצים לשתף מספר רחב ככל האפשר של חברים, עובדים ומנהלים, בארגון ומחוצה לו, בשימוש בתחקירי PCאון. בדומה לטלפון ופקס, ככל שרבים יותר המשתמשים בהם, כך גם גדלה התועלת. אתה ודאי מכיר זאת.

עכשיו אתה מוזמן לקרוא את התחקיר המצורף, להתרשם באופן בלתי אמצעי ולהתקשר - דרך האתר www.pCon.co.il/promo לטלפן 03-9667939, לפקסס 03-9660310 או מייל - sub@pcon.co.il

אחרי שתצטרף ותסתכל קדימה שנה מהיום, יתכן וגם אתה תחשוב כמוהו? מה דעתך?

PCאון ©

למנהלים ומשתמשי מחשב בכירים

תדרוך מקצועי קצר ומרוכז ● בחדשות ומידע שימושי ייחודי ● למיצוי המחשוב באופן מרבי

...והפעם... לנהל סיכונים ביעילות

מסר אישי

כמו המדינה, כך גם הארגון הממוצע, מתפקד בסביבה עתירת סיכונים. המחשוב הוא אחת המטרות העיקריות לסיכונים אלה - קריסת מערכות, נוזקה, שריפות, אסונות טבע. וב**ישראל** - לעולם אינך יודע האם ומתי תמצא את הארגון בחזית. במקביל, ההשלכות של שינויים רבים בעולם העסקי, בטכנולוגיות וברגולציות, מחייבות להתעדכן, כאשר מאד מאד לא מומלץ לדחות למחר את הטיפול בסיכונים האפשריים, בגישת "יהיה בסדר".

מה התחדש בתחום? האם יש מקום לייעול תהליך ניהול הסיכונים בארגונך? האם עדיף לנהל סיכונים בעזרת שירות חיצוני? כל זאת ועוד - בתחקיר הנוכחי.

תמצית החדשות בעולם המחשוב טור

- חדשות בקצרה 3
- הכרזות 3
- ווב 2.0 4
- פריצות דרך 4

תוכן התדרוך השבועי טור

להתמקד בעיקר

- על ERM, ORM ומה שביניהם 5
- הסיכונים החדשים 5
- שינוי התפיסה 6

תועלות, הזדמנויות והיבטי רכש

- הכלכלה שבמשוואה 7
- צא ולמד 7
- מוצרים מסייעים 8

המיוחד ביישומי מחשב בישראל

- שיחות מהשטח 9
- טיפים לניהול סיכונים יעיל 9
- צעדי התמודדות 10

להעמיק בנושאי מפתח

- על חוקים ועל תקנות 11
- מגבלות ואתגרים 11
- מתודולוגיות 12

ליצירת קשר אישי

עורך ראשי - **קובי שפיבק** B.Sc. ,MBA

עורך - **עמית לוי**

תחקיר וכתיבה - **יבגני צ'רקסקי**

טלפון - **03-9667939**, פקס - **03-9660310**

דואר - **ת.ד. 2340 ראשון לציון 75121**

E-Mail - editor@pcon.co.il

לתשומת לבך

- כל הזכויות שמורות **לקומרקטינג בע"מ** ©. אין לצלם או להפיץ את הגיליון ללא היתר ובכל צורה שהיא.
- אנו משתדלים להביא מידע אמין ומדויק אולם האחריות לתוצאות השימוש בו תחול על המשתמשים.
- שמות המוצרים והחברות המוזכרים ב-**PCאון**, הם שמות שמורים של בעליהם.
- ככלל המחירים בגיליון הם בדולרים וללא מע"מ. מחירי ספרים ניתנים בש"ח כולל מע"מ.
- לאתרים **באינטרנט** יש להוסיף הקידומת **http://**

לכבוד **קומרקטינג בע"מ**
פקס 03-9660310
ת.ד. 2340 ראשון לציון 75121

___ כן אני רוצה להיות מנוי **PCאון**, לתקופה של 3 / 6 / 12 חודשים. אני מצרף סך בשקלים של $134 / $254 / $484 + מע"מ (סמן בחירתך בעיגול), לפקודת **קומרקטינג בע"מ** ומחכה לגיליון הקרוב.

שם מלא_____

ארגון_____

תפקיד בארגון_____

כתובת_____מיקוד_____

טלפון_____פקס_____

תאריך_____חתימה_____

הערות _____

PCאון© למנהלים ומשתמשי מחשב בכירים

11.777– חדשות בקצרה

• **בצעד חריג, מפציר המשרד לביטחון פנים של ארה"ב (Department of Homeland Security) במשתמשי חלונות, לעדכן את מערכותיהם ללא דיחוי, עם תיקוני האבטחה האחרונים ממיקרוסופט.** הסיבה: להערכתם, אחת מפרצות האבטחה שאליהן התיקונים מתייחסים, חמורה במיוחד ועשויה להוות סיכון לאומי לתשתיות המדינה. את פרטי הודעת הארגון והמלצותיו, תמצא כאן - www.dhs.gov/dhspublic/display?content=5789

• **Dell** יוצאת בקריאה להחזרת כ-4.1 מיליון סוללות ליתיום-יון למחשביה הניידים, שבמקרים נדירים, עלולות להתחמם ולהוות גורם מסכן להתלקחות אש. הסוללות נמכרו בתאריכים ה-1 ב**אפריל**, 2004, עד ה-18 ב**יולי**, 2006. החברה קוראת ללקוחותיה להתקשר אליה מיידית, בכדי לקבוע האם מבצע ההחזרה רלבנטי עבורם. בינתיים, ניתן להמשיך ולהשתמש במחשבים אלה בבטחה, על ידי כיבוי המחשב, הוצאת הסוללה, ושימוש במתאם AC וכבל חשמל. סקירה רחבה יותר והפניה לדגמים השונים, ראה בחדשות **פיסיאון** - www.pcon.co.il/v5/NewsHeadItem.asp?id0=1168

• בתערוכת **LinuxWorld** שנערכה ב**סן פרנסיסקו**, הודיעה **סאן** כי עד סוף השנה תיפתח עוד שני מודולי **ג'ווה** בפני קהילת הקוד הפתוח - **JavaC compiler** ו-**Hotspot virtual machine**. במסגרת ראיון בתערוכה, אמר נציג **מוטורולה** כי עד 60% מהטלפונים הסלולאריים שלה, ייתבססו בשנים הקרובות על **לינוקס**. **IBM** הודיעה על שת"פ עם **Transitive**, לתרגום תוכנות שנכתבו במקור למעבדי **x86** בהם **IBM** משתמשת, לריצה גם על שרתים מבוססי מעבדי **IBM Power**. **Novell** ו**לנובו** הודיעו על שת"פ לפיתוח מחשב נייד מבוסס **לינוקס**.

12.777– הכרזות

כמה הכרזות חדשות בנוף המחשוב:

• **סאן מיקרוסיסטמס** הכריזה על משפחת האחסון המודולרי **Sun StorageTek**. מערכי הדיסקים מגיעים בתצורת **San** עם **4GB FC Interface Front to End** ותומכים בשילוב דיסקים **SATA-2** יחד עם דיסקים **FC**. על פי החברה, שני הדגמים הראשונים במשפחה מעניקים יחס כפול של צפיפות/נפח על פני שטח נתון ביחס לפתרונות מתחרים, ודגם 6540 מספק ביצועים טובים פי שניים. ☎ 09-9710500.

• ייתכן ונראה דיסקים קשיחים בנפח 1 טרה בייט, עוד השנה! כך אמרו לאחרונה נציגים מ**היטאצ'י** ו**מסיגייט** (ששיחררה דיסק בנפח **750GB** כבר ב**אפריל** השנה).

• **AMD** הציגה גרסה חדשה לשבב ה**אופטרון**, שהיה זה שהכניס אותה בעבר כמתחרה בתחום מעבדי השרתים. דגם **Rev F** תומך בוירטואליזציה ובזכרונות **DDR2**. זהו מעבד כפול ליבה, אך החברה מתכננת להפכו לבעל ארבע ליבות, עד 2007. החל מ-**$749** לדגם 1218 (**2.6GHz**).

• **פוג'יטסו-סימנס** השיקה שרת **Blade** חדש מסדרת **Primergy**, המבוסס על **8** מעבדי **AMD Opteron** כפולי ליבה. השרת משלב דחיסות גבוהה וביצועים רבי-עוצמה, המתאימים לשימוש בחוות שרתים או באפליקציות מבוססות מוקדי שירות. **טק דטה** ☎ 1-800-221-270.

• **Captaris RightFAX** 9.3 היא גרסה חדש לשרת הפקסים **RightFAX**. היא מציעה קישוריות ליישומים ארגוניים כ-**ERP**, התאמה לארגונים המבוזרים במספר אתרים, מהירות גבוהה בהמרת מסמכים, ממשק אינטרנטי ותמיכה בהיערכות למקרה אסון. **סיסטמטיקס** ☎ 03-7660111.

13.777– וב 2.0

מגוון טכנולוגיות ווב 2.0, חידשו לאחרונה:

• שוק ה-**CRM** צמח להיקף של 11.7 מיליארד דולר ב-2005. זו היא עליה של 8% ביחס ל-2004, לה אחראי בין השאר תחום ה-**Hosted CRM**. לפי **AMR Research**, צמיחה זו צפויה להימשך והתחום יגיע השנה להיקף של 12.9 מיליארד דולר.

• **גוגל** רכשה את חברת **Neven Vision**, המתמחה בניתוח תמונות, במטרה להעשיר את תוכנת ניהול התמונות המקוונת שלה **Picasa**. ייחודה של הטכנולוגיה, ביכולת "להבין" את תוכן התמונה (גם אם בקווים כלליים בלבד), על ידי ניתוח ישיר שלה.

• 50 מיליון בלוגים פעילים כיום ב**אינטרנט**! לפי סקר **Technorati**, מדובר בגידול פי 100 בהיקפם, תוך שלוש שנים! ועוד באותו נושא - **מיקרוסופט** הכריזה על גרסת בטא חינמית של כלי עזר לכותבי בלוגים - **Windows Live Writer** המסייעת לערוך בלוגים ולראות כיצד בדיוק יראו, לפני העלאתם הסופית לאתר - windowslivewriter.spaces.live.com

• עריכת תזכורות מקוונות מציע אתר **Rminder**. ניתן להירשם לנסיון ולהתרשמות, לקבלת 8 תזכורות בחודש בחינם - www.rminder.com

• **Meebo** הוא אתר חדש נוסף, המציע שרות בנוסח **Web 2.0**. הרעיון: **Login** חד פעמי, המחבר אותך בבת אחת לכמה שרותי מסרים מידיים. **Meebo** גם הציג לאחרונה **Widget**, המאפשר תקשורת ישירה עם מבקרים באתרך - www.meebome.com

14.777– פריצות דרך

החידושים הבאים מסמנים פריצות דרך מעניינות:

• סטרט אפ בשם **Movidis** מציע שרתים עם 16 ליבות במעבדים. מלבד מספר הליבות הגדול, מיוחדים המעבדים גם בהיותם מבוססי ארכיטקטורת **MIPS**, תכונה שדורשת שימוש ביישומים ייעודיים. המחיר - החל מ-**$3,000** - www.movidis.com

• ב**בריטניה**, הפרסום המקוון כבר עוקף כמה מצורות הפרסום המסורתיות! תחום זה הגיע להיקף של 2.48 מיליארד דולר ב-2005, ולפי שלוש משוק הפרסום ברדיו המקומי. הוא ניצב כעת במקום רביעי בפופולאריות, אחרי פרסום בעיתונים, בטלביזיה ובדיוור ישיר. נתוני **Ofcom**.

• פריצת דרך חשובה עבור פיתוח יישומים ניידים מבוססי **לינוקס**. **Trolltech** הציגה טלפון סלולארי בשם **Qtopia Greenphone**, בעל אפשרויות תכנות מתקדמות. הוא מיועד להיות כלי עזר ייחודי למפתחים, שיאיץ תהליכי פיתוח יישומים ניידים - www.trolltech.com/products/qtopia

• רק לאחרונה נכנסו לשוק מוצרים ראשונים של דור שלישי ברשתות **אינטרנט**, וכבר מדובר על פיתוח "דור רביעי" להתקנים אלחוטיים. **WiMax** עומד במרכז תכנונים אלה והוא יציע יתרונות רבים, כמו מעבר חלק בין אזורים שונים (בניגוד למעבר בין **Hotspots**, בשיטת **WiFi**).

• מעבדות **IBM** הדגימו אחסון על מולקולה בודדת! מדובר בתרכובת אורגנית, בה הצליחו למתג בעקביות בין שתי רמות התנגדות חשמלית, שגם נשמרו בתרכובת לאורך זמן. נפחו הפיזי של "רכיב הזכרון" החדשני (אם כי עדיין נסיוני) - כמאית מנפח רכיב בסיסי לזכרון סיליקון.

21.777 – על ERM, ORM ומה שביניהם

תחום ה-ERM (Enterprise Risk Management), מתחלק לפחות לשלושה תחומי משנה: ORM (או Operational Risk Management), סיכוני אשראי וסיכוני שוק. ה-**ORM** (ניהול סיכונים תפעוליים) עוסק בכל הסיכונים הנובעים מהפעילות התפעולית היומיומית בחברה. בין השאר, **ORM** כולל סיכונים הנובעים מכשלי מערכות (כולל מערכות מחשוב), מתהליכים עסקיים לקויים (פנימיים וחיצוניים), כשלים אנושיים והונאות. הפיכת המנמ"ר המודרני לגורם מרכזי בניהול העסקי והכלכלי של הארגון, מכניסה גם את נושא הכשלים העסקיים לתחום אחריותו. מעורבות המחשוב המתרחבת, בשגרת יומו של העובד הממוצע, כמו גם היקפן הגדל של מחלקות המחשוב עצמן, הופכים גם את נושא הסיכונים ממקור אנושי, לרלבנטיים מתמיד עבור המנמ"ר.

עקרונית, ניהול סיכוני מחשוב ואבטחת מידע הוא תחום שנכלל ב-**ORM**, אך באופן מסורתי מקובל לעיתים להתייחס אליו, כאל תחום נפרד שמושך אליו תשומת לב מיוחדת. עד לא מזמן, ארגונים בארץ נהגו לייחס את מירב תשומת הלב שלהם לניהול סיכוני מערכות מידע. סקרי הסיכונים שבוצעו עסקו בעיקר בבדיקת מערכות האבטחה בארגון. מסיבה זו, עדיין מקובל לראות בניהול סיכונים, גם אם הכוונה היא לסיכונים שלא נובעים באופן ישיר ממערכות המחשוב, תחום בעל זיקה ישירה למחלקת ה-**IT** בארגון. עם זאת, היום ניתן להבחין בכך שארגונים מתחילים לייחס תשומת לב, גם לניהול הסיכונים האחרים (תפעוליים, פיננסיים ועסקיים). גורם משמעותי המניע ארגונים לעסוק ב-**ORM** דווקא בתקופה האחרונה הן דרישות הרגולציה הרבות (ראה ידיעה 51). לכך נוספות התפתחויות בעולם העסקי, בטכנולוגיות שונות ובעבודה במודלים חדשים כמו מיקור חוץ, שמשנים את תמונת המחשוב ולכן גם את הסיכונים הכרוכים בו.

ניהול סיכונים אינו דבר פשוט והוא צופן בחובו מגוון אתגרים, בהם אתגרי קבלת משאבים מתאימים לטיפול בנושא זה ואתגרי איסוף נתונים ובניית מדדים סטטיסטיים. **בישראל** במיוחד, נכנסים לתמונה סיכונים יוצאי דופן, כתקיפות טרור, מקוון ופיזי - בעקבות המלחמה בצפון, מצאו מנמ"רים רבים באזורים אלה את תכנית ההתאוששות מאסון שלהם, בין אם הייתה קיימת או לא, עומדת ל"בוחן פתע" חריף ומתמשך. לקריאת דוגמא מאלפת מהשטח, באתר **פיסיאון** - www.pcon.co.il/v4/interviews.asp?ty=1&id_m=116

לפי סקר **BSA/ISSA**, הרבה השתנה מבחינת אימוץ ניהול הסיכונים והמוכנות לסיכונים בארגונים מאז שנת 2003. ב-93% מהארגונים קיימת מדיניות אבטחה (המספר עלה מ-72%), ב-91% מהארגונים קיימות בקרות גישה (עלה מ-73%) ב-91% מהארגונים קיים אדם מוגדר האחראי על אבטחת מידע (עלה מ-78%). מצד שני, בסקר ארגון **IT Governance Institute** בין 200 מקצועני מחשוב מ-14 ארצות, נמצא כי פחות מרבע מהארגונים בודקים בקביעות סיכונים ממקור חיצוני, ורק בשליש מהמקרים עוברת תכנית ניהול הסיכונים במחשוב תהליך אישור של ההנהלה.

<u>לסיכום - אין ספק כי ניהול סיכונים הוא תחום שהמנמ"ר חייב להכיר וליישם, לשרידות עסקית ואבטחת מערך המידע. לאור ההתפתחויות בתחום, מומלץ להתעדכן ולהתכונן.</u>

22.777 – הסיכונים החדשים

בשנתיים האחרונות השתנתו תמונת והיקף הסיכונים מולם מתמודד הארגון, מכמה סיבות:

• **שינוי התפיסה בהגדרת תפקיד המנמ"ר** - ממנהל טכני הופך המנמ"ר למנהל עסקי וכלכלי. שינוי זה, גורם למנמ"רים לשנות תפיסה ולהתייחס לסיכונים (עסקיים וכלכליים) רבים ומגוונים מתמיד.

• **תמורות בעולם העסקי** - עולם העסקים מחייב הסתכלות על סיכונים בפרספקטיבה רחבה יותר ובהתאם לכך, התייחסות למספר סיכונים רב מתמיד. ארגונים "התבגרו" בגישתם לנושא ומתייחסים אליו כעת באופן נרחב יותר. זאת, בשונה מהעבר, כשהמנמ"ר התייחס בעיקר לסיכוני מחשוב בולטים, כמו וירוסים, **SPAM** וחדירת האקרים.

• **מיקור חוץ** - ארגונים רבים נוהגים להוציא פרויקטים, שירותים, תוכנות, מערכות, עובדים ואף מחלקות שלמות למיקור חוץ. מחד, מיקור חוץ דורש מהארגון לכאורה, לעסוק ולהיות מעורב בפחות תחומים ולכן מפחית סיכונים. מאידך, עצם קיום היחסים עם ספק מיקור החוץ, מציג סיכונים חדשים, אליהם חייב הארגון להתייחס. למשל - אמינות הגורם החיצוני במתן השרות או הוצאת מידע רגיש מחוץ לארגון.

• **חידושים טכנולוגיים** - מציגים בקביעות סיכונים חדשים, להם חשוב להיות מודע. להמחשה: הרשתות האלחוטיות מציגות סיכוני אבטחה ידועים. **VoIP** נמצא כעת במצב בו ידוע שהוא חשוף להאקינג, אך התקיפות עוד בחיתוליהן ועוד יותר מכך, הפתרונות. ובמבט לעתיד: טלפונים סלולאריים צוברים "חוכמה", המבשרת על עליה בפוטנציאל העסקי שלהם, לצד עליה בפוטנציאל הסיכון.

• **רגולציה** - במגוון תחומים כמו הנהלת חשבונות, בנקאות, ביטוח ושירותי בריאות, מתעדכנות דרישות רגולציה, המחייבות לנהל סיכונים הכרוכים בעיסוקים אלה. ידוע גם **SOX**, המחייב ארגונים רבים העובדים גם **בארה"ב** או מול חברות **בארה"ב**.

23.777 – שינוי התפיסה

אלה כמה השלכות מעשיות, להן הביאו החידושים והמגמות בניהול הסיכונים:

1. **היקף סקרי הסיכונים** - רוב סקרי הסיכונים שהזמינו בעבר (עד לפני כ-3 שנים), היו בעיקר בתחום אבטחת המידע. ההמלצות שסקרים אלה הניבו היו בעיקר הוספת אנטי-וירוסים ו-**Firewalls**. היום, הראייה היא יותר מערכתית. מבצעים ניהול סיכונים גם ברמה העסקית. למשל - הסיכון ביציאה לשוק עם אתר **אינטרנט** שאינו מאובטח דיו, לעומת הסיכון שהמתחרים יצאו עם אתר דומה קודם לכן.
2. **מיקור חוץ** - מערכות היחסים עם ספקי מיקור החוץ דורשת לתת לספקים גישה למערכות המידע בארגון. יצירת קשרים אלה היא בדרך-כלל מוכוונת משימה ולוקה בחסר מבחינת גישה מובנית לאבטחת מידע. אבטחת ממשקים אלה נחוצה בכדי להפחית סיכונים הכרוכים במיקור חוץ. הספק עצמו ובפרט האנשים העובדים אצלו, עלולים להוות גורם סיכון. הפחתת סיכון זה יכולה להתבצע על-ידי מעורבות בבחירת העובדים שיטפלו בארגון אצל ספק מיקור החוץ. הוצאת מיקור חוץ לחו"ל, דורשת התייחסות ספציפית לסיכונים האופייניים למדינות אלה, דוגמת סיכוני אסונות טבע.
3. **התמודדות עם טכנולוגיות חדשות** - סיכונים "טכנולוגיים" כמו שימוש בשיחות **VoIP** או רשתות אלחוטיות, מחייב ביצוע סקר סיכונים כאשר מכניסים טכנולוגיות אלה לארגון. במידה ועלות ההתגוננות עולה על התועלת מהשימוש בטכנולוגיה, יש לשקול שנית את עצם השימוש בה.
4. **הגדרת אחריות** - כאשר הארגון ניהל סיכוני **IT** בלבד, האחריות הייתה על המנמ"ר. היום קיימת נטייה להגדיר גוף כלל ארגוני, שיהיה אחראי על ריכוז וניהול כל הסיכונים. לפעמים מדובר באחד הסמנכ"לים ולפעמים במנהל בלתי תלוי.

31.777 – הכלכלה שבמשוואה

כבר ב-2005, 66% ממקבלי ההחלטות בארגונים, התכוונו להגדיל השקעות בניהול סיכונים בשלוש השנים הבאות (סקר Ernst & Young). אין ספק שיש הבנה לנחיצות הנושא ומעצם הגדרתו, ניהול סיכונים היא פעילות בעלת השלכות משמעותיות לצמצום הפסדים ונזקים כלכליים. עם זאת, פעילות זו עצמה, דורשת השקעה של כספים וזמן, שההנהלה לא תמיד ששה לאשר. לאור זאת, לא מפתיע לגלות, כי 71% מהארגונים **בארה"ב** מטפלים בנושא ניהול הסיכונים באופן לא מסודר (סקר **Mercury Interactive**). נתונים נוספים, ממחישים, עד כמה גישה זו איננה "רעיון טוב": לפי **Infonetics Research**, עלות **Downtime** של מערכות מחשוב לארגונים גדולים **בארה"ב**, היא בממוצע 3.6% מרווחיהם השנתיים, כאשר אצל ארגונים יצרניים מדובר ב-9% ואצל ספקי שירותים פיננסיים מדובר ב-16%.

מובן שלא לכל סיכון ניתן להתייחס, מסיבות תקציביות. ניסיון להתייחסות מלאה לכל הסיכונים, כולל בעלי סיכוי ההופעה ורמת הנזק הקטנים יחסית, תעלה את רמת ההוצאות התפעוליות בחברה, לרמה בה היא תפסיק להיות רווחית. האומנות בניהול סיכונים יעיל, טמונה בידיעה לאילו סיכונים להתייחס ומאילו עדיף להתעלם. דרך העבודה המקובלת היא מיפוי 10% מהתהליכים בארגון בהם זורמת כמות הכסף הרבה ביותר. בתהליכים אלה מחליטים אילו סיכונים לנהל, על פי סיכוי התרחשות ומידת הנזק הצפויה.

אבטחה היא כיום נושא מרכזי גם בהוצאות ארגונים (ראה עוד ב**תחקיר 758 - ROSI - כמה להשקיע באבטחה?**) וגם בניהול סיכוניהם. על פי **SANS Institute**, אבטחה איננה נושא אסטרטגי בארגון, אם איננה משולבת בניהול סיכונים. לפי סקר שנערך על-ידי ארגון ה-**BSA** (או **Business Software Alliance**) בשיתוף עם ה-**ISSA** (או **Systems Security Association**), 76% מהארגונים מכירים בעובדה שהעלאת העדיפות שניתנת לאבטחה, הופכת את הארגון ליעיל יותר ומקנה לו יתרון תחרותי על-פני המתחרים. נתון זה מבהיר עד כמה נושא ניהול סיכוני האבטחה משמעותי לארגונים בסביבה תחרותית. להמחשה, נניח ששתי חברות מתחרות מנהלות חנויות **אינטרנט**, כשלכל אחת מחזור מכירות העומד על **$20,000** ליום. אם שני האתרים מותקפים על ידי האקרים, ורק אחת מהן התכוננה לסיכון זה, לחנות שלא התגוננה צפוי הפסד מיידי של **$20,000** ליום. לכך יש להוסיף נזק כלכלי מאובדן מוניטין, שכן הלקוחות שנתקלו בתופעה עלולים לעבור לחנות המתחרה ואף נזקים מפריצה למידע עסקי או לפרטי לקוחות. לפי אותו הסקר, 59% ממומחי האבטחה חוששים ממתקפת **אינטרנט** מהותית בשנה הקרובה, אך רק 73% מאמינים שהם מוכנים היום למתקפה כזאת, טוב יותר מאשר לפני שנה.

32.777 – צא ולמד

אלה כמה מקורות להכשרות בניהול הסיכונים:

• **שיא סקיוריטי** - מתפקדים כבית-ספר לאבטחת מידע. מלמדים ארגונים לבצע ניהול והערכת סיכונים בהיבט מערכות המידע - הדגש הוא על אבטחת מידע, סיכוני נזק, גניבה ופגיעה. מבצעים סקרי סיכונים בארגונים קטנים ובינוניים. ☎ 054-5222305.

• **ל.ה.ב** - מציעה הכשרת מנהלי סיכונים עם הסמכה מקצועית מטעם ארגון ה-**PMI** (או **Project Management Institute**). היקף הלימוד הוא 40 שעות והעלות היא 1,260 ש"ח. ☎ 03-6407775.

• **ה-IIA (Institute of Internal Auditors)** - מציע הסמכה הנקראת **CIA (Certified Internal Auditor)**. התוכנית וההסמכה מכשירות מבקרי פנים. דרישות הקבלה - תואר ראשון. בסילבוס התוכנית נכללים תכנים רבים הקשורים להערכת סיכונים, ניהול סיכונים ומיפוי סיכונים ארגוניים. ל-**IIA** קיימת נציגות בארץ, תחת השם **לשכת המבקרים הפנימיים ישראל**. גם בחינת ההסמכה מוצעת **בעברית**. לפרטים ☎ 03-5610933.

33.777 – מוצרים מסייעים

השרותים והמוצרים שלהלן יעזרו לנהל סיכונים:

• **דן אנד ברדסטריט** - מציעה כלי תוכנה שונים, המיועדים לסייע בניהול סיכונים. ☎ 03-7330330.

• **הלפרין שירותי יעוץ** - מציעה שרותי ייעוץ לניהול סיכונים (תפעוליים, אשראי ושוק) וגם סקרי סיכונים, כולל הערכת סיכונים ומסמכי מדיניות. ☎ 03-5224402.

• **מטאור** - מציעה ייעוץ לניהול סיכונים במגוון תחומים, כולל מתודולוגיות ייחודיות לניהול סיכונים בתהליכי מיקור-חוץ ובפרויקטי פיתוח. ☎ 03-5783520.

• **מתודה** - מציעה את **נוהל מפת"ח** (ראה **777.53**), שרות ניהול סיכונים תפעולי וסדנאות ניהול סיכונים לארגונים (ללימוד כללי של הנושא או לאיתור סיכונים בפרויקט ספציפי). מחיר יום הדרכה - כאלף דולר. ☎ 03-6133336.

• **קסלמן פתרונות בניהול סיכונים PwC** - מבצעת סקרי סיכונים, ייעוץ והטמעה. בין השאר, מבצעת התאמה לרגולציות, ביקורת פנים ופיתוח תוכניות עבודה ליחידות ביקורת פנים. מציעה גם את כלי העזר לניהול סיכונים **TeamMate** ($11,000 ל-5 משתמשים). ☎ 03-7954850.

• **Comsec** - חברת ייעוץ המתמחה באבטחת מידע. מציעה הערכת סיכונים בכל הרמות. ☎ 03-9234646.

• **iTcon** - שירותי הייעוץ שלה בתחום ניהול הסיכונים מסתמכים על תהליך שלם, הכולל ניתוח סיכונים וזיהוי פערים לעומת נקודות חזקות. ☎ 03-6490039.

• **Secoz** - מספקת סקרי סיכונים והערכת סיכונים, לצד פתרונות אבטחה והקטנת הסיכונים העסקיים בארגונים, תוך התמקדות ביעדים אסטרטגיים ☎ 08-9716605.

• **TeraData** - מציעה מגוון מוצרים עם יכולת לנהל סיכונים, כולל מוצרי ניהול פיננסי, ניהול שרשרת אספקה וניהול קשרי לקוחות. **י.א. מיטווך** ☎ 03-5265555.

• **IBM** - מציעה מוצרי תוכנה לניהול סיכונים ולהתאמה לדרישות רגולציה (כמו **SOX**). ☎ 03-9188111.

777.41– שיחות מהשטח

שוחחנו עם 3 מומחי ניהול סיכונים, ולהלן דבריהם:

שי זנדני, מנכ"ל **קסלמן פתרונות בניהול סיכונים PwC** (☎ 03-7954850), אומר שלרגולציה יש השפעה גדולה על העיסוק בניהול סיכונים, כיוון שהיא מחייבת לעשות זאת. ניתן לומר, שרגולציה באה בגלים ועכשיו אנחנו נמצאים על אחד הגלים הללו. גם חידושים במגמות שוק יוצרים סיכונים חדשים, ומחייבים ארגונים לעסוק בהם - כך למשל נושא ה-**Outsourcing** או ה-**Off-Shoring**. כל מגמה ושינוי כזה, יוצרים סיכונים חדשים אליהם יש להיערך. עולם הבנקאות למשל, עבר שינוי משמעותי ביותר מבחינת התקדמות טכנולוגית ב-10 השנים האחרונות והיום הוא מתקדם מאוד במתן שירותים מתוחכמים ב**אינטרנט**. התקדמות זו יצרה סיכונים חדשים, בעולם שהוא יחסית שמרני. מנהל סיכונים פנימי הוא בעל הכרות טובה עם מבנה הארגון, תהליכיו, סיכוניו וצרכיו ובזה יתרונו. יועץ חיצוני, לעומת זאת, יכול לתת לארגון פרספקטיבה חיצונית ולהראות מה קורה בארגונים דומים אחרים.

לפי **קרן אלעזרי**, ארכיטקטית אבטחת מידע ב-**iTcon** (☎ 03-6490039), מומחה ניהול סיכונים פנימי לעיתים אינו אובייקטיבי, כיוון שהוא עלול להיות מושפע מנסיבות "פוליטיות" בארגון. יועץ חיצוני יהיה אובייקטיבי יותר. סיכונים חדשים נוצרים לעיתים כתוצאה מכניסת טכנולוגיות חדישות לארגון. חידושים טכנולוגיים אלו, הם לעיתים חדישים מכדי שיהיה מענה מוכן מפניהם, בדמות של עדכון אבטחה או מוצר הגנה ייעודי. קיימים בשוק מספר כלי תוכנה, שאמורים לעזור בתהליך ניהול סיכונים והם עוזרים בעיקר לארגן מידע שנאסף ולהעריכו. עם זאת, קיים בשוק צורך ממשי בכלי תוכנה שיוכל לעבוד ברמה הבאה, שפירושה לאסוף נתונים ממערכות הארגון באופן אוטומטי ולבצע הערכת סיכונים על פי מידע זה.

איתי ויסברג, מנמ"ר **הכשרת הישוב** (☎ 03-7962262), סבור שהמודעות לתחום ניהול הסיכונים חודרת בשנים האחרונות עמוק לתודעת הארגונים. הרגולציה חודרת אף היא ומגדירה דרישות ברורות לתחום ניהול הסיכונים. **הכשרת הישוב** נמצאת עכשיו בתהליך התאמה להנחיה 104 לחברות הביטוח (המהווה הרחבה להנחיה 357 לבנקים). במסגרת התהליך, הארגון צפוי לקלוט כלי עזר לניהול סיכונים, לכתוב נהלים ולאמץ מתודולוגיה. **איתי** אומר שכמנמ"ר הוא מתעסק בסיכוני ה-IT בלבד, לסיכונים האחרים הוא נחשף כחבר הנהלה. הארגון נמצא כרגע בתהליך שבו מוקמת פונקציה כלל ארגונית שתופקד על ניהול סיכונים, כשכרגע הדבר מרוכז על-ידי המשנה למנכ"ל. **איתי** מעריך שכאשר תהיה בארגון פונקציה כלל ארגונית כזו, הסיכונים עדיין ינוהלו על-ידי כל מחלקה בנפרד אך יהיה דיווח מרכזי, שיראה תמונה רחבה יותר. לדעתו, האתגר המרכזי בניהול הסיכונים הוא מיפויים ודירוגם בצורה נכונה, כשהטיפול בסיכונים הוא בעיה משנית.

777.42– טיפים לניהול סיכונים יעיל

להלן מספר עצות שיעזרו לך לנהל סיכונים ביעילות (על פי CIO.com):

• **למצוא השראה** - ניהול סיכונים דורש לחשוב על הגרוע מכל. הוא דורש לחשוב בפסימיות ולהתכונן למצבים שכל אחד מקווה שלא להגיע אליהם. על-מנת לעסוק בכך, מנמ"רים זקוקים להשראה. מנמ"ר **צי ארה"ב דייב ונייגרן** למשל, מוצא השראה בכך שחיי טייסים וחיילים תלויים במערכת התקשורת שארגון ה-IT שלו מספק.

• **הגדרת מסר ברור** - ניהול סיכונים לא יכול להתבצע על-ידי המנמ"ר לבדו. דרושה לכך מודעות ונכונות לשיתוף פעולה מכלל הארגון. לכן חשוב לחדד מסר, המסביר מדוע ניהול סיכונים הוא כה חשוב לארגון כולו ולמטרותיו העסקיות.

• **גמישות** - לא כולם מבינים מהי החשיבות הגלומה בניהול סיכונים. אחדים כלל לא יבינו מהו ניהול סיכונים. על-מנת להעביר מסר חשוב זה לעמיתים בארגון, כדאי לפעמים לנקוט בגישה עקיפה, שתדגים לכל אחד כיצד סיכונים משפיעים על הפעילות העסקית בפן הספציפי שלו.

• **לצאת מהמשרד** - ניהול סיכונים יעיל כרוך, בין היתר, ביחסי אנוש טובים. לעובדים רבים יש נטייה להתעלם ממתודולוגית ה-ERM הנהוגה בארגון ולחשוב על סיכונים רק בדרך בה הם רגילים. עובדה זו, נכונה במיוחד בתרבות העסקית והחברתית המאפיינת את ישראל (גישת ה"יהיה בסדר"). חשוב להיפגש עם עמיתים, מנהלי המחלקות האחרות בארגון, לבדוק האם הם מנהלים סיכונים בצורה התואמת להשקפת הארגון והאם הם מביאים נכונות להתמיד בכך.

• **להיות "אזרח למופת"** - על-מנת שהמחלקות האחרות בארגון ינהלו סיכונים בצורה יעילה ונכונה, חשוב להוות דוגמה למופת. ודא, שגף ה-IT, המוביל את ניהול הסיכונים בארגון, בעצמו מנהל סיכונים כראוי.

777.43– צעדי התמודדות

ההמלצות שלהלן, יעזרו לייעול תהליכי ניהול הסיכונים:

1. **החלטה על גישת ביצוע** - יש להחליט אם להיעזר בחברה חיצונית לביצוע סקרי הסיכונים או להחזיק בארגון מומחה סיכונים פנימי (ברמה מחלקתית או ארגונית).
2. **הקמת משרד מנהל סיכונים** - על-מנת לבצע ניהול סיכונים באופן מתמיד, רחב ויעיל, רצוי להקים משרד מנהל סיכונים ולהעסיק עובד או צוות עובדים, שתפקידם לעסוק בניהול סיכונים. כאשר קיים משרד ניהול סיכונים ברמה הארגונית, תפקיד המנמ"ר הוא זיהוי סיכונים בתוך מחלקת ה-IT בלבד.
3. **ראייה כלל ארגונית** - שילוב ניהול סיכוני IT בניהול הסיכונים הכלל ארגוני. מחלקת ה-IT, משאבי האנוש והמחלקות האחרות, רואות סיכונים בפרספקטיבות שונות. לכל מחלקה יש מדדים משלה וכלי מדידה משלה ויתכן שחלק מהמחלקות בארגון כבר מנהלות סיכונים באופן חלקי. לכן, חשוב שניהול הסיכונים יתבצע ברמה הכלל ארגונית על-פי כללים, מדדים ומתודולוגיה כלל ארגונית.
4. **שקילת סיכונים הדדיים** - כאשר הסיכונים מנוהלים ברמה המחלקתית בלבד, יש נטייה להתייחס לנזק העלול להיגרם לאותה המחלקה בלבד. עם זאת, ניהול הסיכונים ברמה הכלל ארגונית, מחייב להסתכל על הנזק שסיכוני כל מחלקה עלולים לגרום למחלקות האחרות ולארגון כולו.
5. **ראיית השורה התחתונה** - בבואך להעריך מהו הנזק הפוטנציאלי שסיכון עלול לגרום, אין להסתכל רק על הנזק המיידי אלא גם על הנזק הכולל והעקיף בטווח הקצר והארוך.
6. **תוצר ניהול הסיכונים** - תוצר ניהול הסיכונים הוא המלצות. ההמלצות יכולות להיות "טכנולוגיות" (כמו התקנת Firewall נוסף) או המלצות או"ש (ארגון ושיטות).
7. **ניהול סיכונים לטווח הארוך** - לאורך זמן, חלק מהסיכונים הופכים להיות לא רלוונטיים וסיכונים חדשים נכנסים לתמונה. על הארגון להיערך ולהתאים עצמו לכך, בהתמדה.

51.777 – על חוקים ועל תקנות

לעתים, ארגונים נדרשים לבצע ניהול סיכונים גם על-פי חוקים ותקנות שונות, כולל:

• **SOX (Sarbanes-Oxley)** - אוסף תקנות ידוע זה, מחייב קיום בקרות במערכות המידע בארגון, שמפיקות בסופו של דבר דו"חות כספיים. החידוש העיקרי בו, מבחינת ניהול סיכונים, היא האחריות האישית שהוא מטיל על ה-**CEO** וה-**CFO**, והענישה החמורה שמוגדרת בו - עד 20 שנות מאסר וקנס של עד 5 מיליון דולר. ראה גם **תחקיר 712 - מסרבנס-אוקסלי למנמ"ר**.

• **הוראה 357 של בנק ישראל** - זוהי הנחייה לניהול בנקאי תקין, שפורסמה על-ידי **המפקח על הבנקים**. **הוראה 357** מגדירה הנחיות לגבי האופן שבו יש לנהל מערכות מידע בארגון, כולל התייחסות לביצוע סקרי סיכונים תקופתיים, הערכות לגיבוי והתאוששות והנחיות לגבי מיקור חוץ.

• **הוראות באזל** - הוראות **ועדת באזל** נחשבות להנחיות מחייבות בעולם הבנקאות האירופאי והישראלי. מדובר בתקן שפורסם על-ידי ה-**BCBS** (או **Basel Committee on Banking Supervision**), המתייחס בין השאר להתמודדות הארגון עם סיכונים תפעוליים.

• **תקן 7799** - התקן נכתב במקור על-ידי ארגון התקינה הבריטי, ומאוחר יותר אימץ אותו ארגון **ISO** כתקן **ISO1799**. **תקן 7799** עוסק באבטחת מידע מנקודת מוצא ניהולית ולא טכנית. התקן מדבר על מספר מעגלי אבטחה - אבטחה פיזית, אבטחת רשומות, מהימנות עובדים ואבטחת ממשקים עסקיים. נקודה מרכזית בו, היא ההתייחסות לניהול סיכונים, כבסיס לאבטחת מידע.

52.777 – מגבלות ואתגרים

מספר גורמים עלולים לעכב תהליכי ניהול סיכונים בארגון:

• **אופטימיות מוגזמת** - סיכונים בכלל וניהולם בפרט הינם דברים שלאף-אחד אין רצון רב להתעסק בהם. עובדה זו נכונה במיוחד במציאות הישראלית, בה גישת ה "סמוך" / "יהיה בסדר" מתבטאת גם בעולם העסקים.

• **מחסור בנתונים סטטיסטיים** - ניהול והערכת סיכונים מתבססים כמעט תמיד על ניסיון העבר, ניסיון חברות אחרות ונתונים סטטיסטיים שונים. לא לכל סיכון אליו רוצים להתכונן קיימים הנתונים הסטטיסטיים המאפשרים לקבוע מהו סיכוי התרחשות הסיכון ומה היקף הנזק שהוא צפוי לגרום. מצב זה מסבך את ניהול הסיכונים, כמו במקרה של התמודדות עם סיכוני טכנולוגיות חדשות.

• **מציאות עסקית תחרותית** - עולם העסקים, ברוב הענפים, הוא תחרותי ביותר. תחרות אינטנסיבית זו מציבה בפני הנהלת הארגון בדרגים השונים דרישה לספק **TTM (Time to Market)** מהיר ביותר. יש דרישה להשיק שירותים חדשים ומוצרים חדשים באופן מהיר, על-מנת להקדים את המתחרים ולעיתים נדרשים להתעלם מסיכונים פוטנציאליים, פשוט כי אין זמן להיערך אליהם.

• **המציאות הביטחונית במדינת ישראל** - **ישראל** נמצאת במציאות ביטחונית, בה העולם העסקי והפיננסי מושפע גם מאירועים מדיניים וביטחוניים. סיכוני טרור העלולים, חלילה, לפגוע בעובדי הארגון, במוסדותיו, משרדיו ולקוחותיו הם סיכונים מגוונים, חמורים ומשתנים, שלא פשוט ולא זול להיערך אליהם.

• **סיכונים הטמונים בניהול הסיכונים עצמו** - לדוגמא - הוצאות ניהול סיכונים הפוגעות ברווחיות פרויקט או ניהול סיכונים שלא לוקח בחשבון פעילויות אחרות בארגון וכך גורם לקונפליקט בין משאבים.

דגש – סיכונים בקישורים

להלן מספר מקורות להעשרת הידע בתחום:

• **RMA - Risk Management Association** - ארגון מקצועי למנהלי סיכונים, העוסק גם בסיכונים תפעוליים - www.rmahq.org/RMA

• **IRM - The Institute of Risk Management** - ארגון העוסק בתחום ניהול הסיכונים ומציע הסמכות בתחום - www.theirm.org

• **Risk Management Magazine** - אתר אמריקאי העוסק בניהול סיכונים וכולל כתבות שונות בנושא זה - rmmag.com

53.777 – מתודולוגיות

קיימות גישות ומתודולוגיות רבות לניהול סיכונים, ובהן:

• **נוהל מפת"ח** - הנוהל פותח על-ידי חברת **מתודה** מחשבים בשיתוף עם מדינת **ישראל**. הוא מהווה נוהל מחייב במגזר הציבורי ומיושם גם במגזר הפרטי וכולל פרק בנושא ניהול סיכונים בפרויקטי מחשוב. מדובר על גישה כוללת למחזור חיי מערכות מידע בארגון. הנוהל מתייחס, בין היתר לשלבי הייזום והאפיון, עיצוב ובניה, תפעול, תחזוקה ותחקור. עבור מנהל הפרויקט הוא מכיל כלים לניהול סיכונים, ניהול סקרים וחישוב אומדן עלויות.

• **Cobit (או Control Objectives for Information and related Technology)** - זהו **Framework** לניהול **IT**, שנוצר על-ידי ה-**ISACA** (או **Information Systems Audit and Control Association**) וה-**IT Governance Institute**. **COBIT** מדבר על 3 תחומים - תכנון וארגון, רכישה ויישום, אספקה ותמיכה וניטור והערכה. עוד הוא מספק, אינדיקאטורים ושיטות מדידה לניהול סיכונים בתחומים אלה.

• **EESA (End to End Security Assessment)** - זוהי מתודולוגיה שפותחה על-ידי חברת **iTcon**. המתודולוגיה מאפשרת הערכת סיכונים בארגון, מנקודת ראות התהליכים העסקיים, בצורה המשקללת את כל המערכות והתשתיות בארגון וכן יחסים בין המערכות והתשתיות ובינן לבין עצמן.

• **COSO II** - מתודולוגיה שפותחה על-ידי **PwC** לפי הזמנת ארגון **COSO**. המתודולוגיה מהווה בסיס ליישום רגולציות כמו **SOX**. ה-**COSO II ERM** מגדיר שלושה מימדים, כשהמימד הראשון מבטא 4 קטגוריות - אסטרטגיה, תפעול, דיווח והתאמה. במימד השני מוגדרים 8 מרכיבים הקשורים זה לזה במסגרת ניהול הסיכונים הארגוני. המימד השלישי מבטא את היכולת להתייחס לכל יחידה במבנה הארגוני.

• **Octave (או Operationally Critical Threat, Asset, and Vulnerability Evaluation)** - זוהי שיטת תכנון והיערכות אסטרטגית המבוססת על ניהול סיכונים. הרעיון הוא לשלוף ולרכז ידע מגורמים רבים בארגון, על-מנת לזהות סיכונים ולבנות אסטרטגיית אבטחה. **Octave** מדבר על שלושה מימדים - הטכנולוגיה, הסיכון התפעולי והאבטחה.