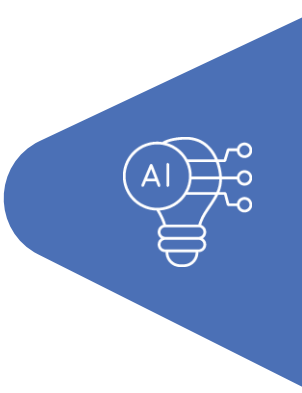

אוניברסיטת רייכמן
FORE
לימודי חוץ
והכשרת מנהלים

קורס ניהול סיכוני סייבר 2026

ניהול אקדמי: ד"ר יוני בירמן

תאריך פתיחה: 08.09.26
8 מפגשים 17:00-21:00

המפגשים יערכו אחת לשבוע בימי ג'*
בשעות 17:00-21:00

תאריכי המפגשים:
8.9.26 • 15.9.26 • 6.10.26 • 13.10.26 • 20.10.26 • *28.10.26 • 3.11.26 • 10.11.26

* מפגש מס' 6 יערך ביום רביעי 28.10.26

ניהול סיכוני סייבר

ההזדמנות להוביל את הארגון שלך עם הבנה מקיפה, כלים אסטרטגיים וחדשנות, בתחום ההגנה בסייבר

בעידן שבו איומי הסייבר הולכים ומתרחבים, אחריות ההנהלה ומקבלי.ות ההחלטות בארגונים להבטחת ההגנה על מידע, תשתיות ותפקוד רציף של הארגון, הופכת להכרח אסטרטגי.

קורס ניהול סיכוני סייבר 2026 מעניק למנהלים ידע מקיף, כלים מעשיים ויכולת הובלה בתחום הקריטי של אבטחת מידע והגנת סייבר. בעידן הדיגיטלי החשיבות של הגנת סייבר גוברת יום ביומו. איומי הסייבר מתרבים ונעשים מתוחכמים יותר, באופן המשפיע על ארגונים בכל הגדלים ובכל הענפים.

עבור מנהלים.ות, האחריות להבטיח את אבטחת המידע, המערכות, הרציפות התפקודית והמוניטין של החברה היא חיונית. החלטות ההנהלה בתחום סיכוני הסייבר יכולות לקבוע את הצלחתו של הארגון בטווח הארוך. הקורס מעניק למנהלים הבנה מקיפה בתחומים השונים של ההגנה בסייבר ומקנה מיומנות חיונית לניהול איומי הסייבר של היום.

במהלך הקורס, המשתתפים ילמדו ויכירו טכנולוגיות ותחומים שונים בהגנה בסייבר כגון:

• ניתוח והבנה של סיכוני סייבר והיערכות ומוכנות אפקטיבית לקראתם.

• היכרות והבנה של האיומים העתידיים, וביניהם מתקפות בינה מלאכותית, כופרות, ודיוג (פישינג).

• הכרת הממשקים בין מערכי סייבר לאומיים לתעשייה.

• הבנת רגולציות, אחריות משפטית וביטוחי סייבר לצורך קבלת החלטות ארגוניות באופן מקיף ורחב.

• הכרת דרכי התמודדות עם משברי סייבר ובניית תרבות ארגונית בטוחה.

• הובלת טרנספורמציה דיגיטלית בטוחה המבוססת על חדשנות טכנולוגית: בינה מלאכותית, ענן ו-IoT.

• אסטרטגיות לבניית ארגון חסין ובטוח.

המפגשים יהיו מורכבים משלושה חלקים: סקירה אקדמית מקיפה של מומחים מעולם התוכן, מקרי בוחן ודוגמאות מהפרקטיקה, ולבסוף הצגת כלים טכנולוגיים על ידי נציגים מחברות מובילות ברמה הבינלאומית.

ההרצאות בקורס יועברו על ידי מומחים ובכירים מגופי תעשיית הסייבר בישראל, לרבות מערך הסייבר הלאומי, הרשות להגנת הפרטיות, אנשי CISO בחברות מובילות, עו"ד ומומחים, מנהלי משברים, חברות ביטוח, וכן בכירים בחברות סייבר מובילות, ביניהן: CheckPoint, Panorays, Anecdotes Spikerz, Cyberready BigID, Sygnia Cytactic ועוד.

הקורס מיועד למנהלים.ות ומקבלי.ות החלטות בארגונים ללא רקע טכנולוגי, מתוך הבנה שהיערכות לסיכוני סייבר בעידן הנוכחי היא הכרחית, ולאנשי הטכנולוגיה בארגון שצריכים להבין את ההיבטים הניהוליים הכוללים וההשלכות של האירועים הטכנולוגיים על החברה.

ניהול סיכוני סייבר

ניהול אקדמי

ד"ר יוני בירמן מומחה באבטחת מידע ובינה מלאכותית. עוסק בהובלה וניהול של מחקר ופיתוח בתעשייה ובאקדמיה בממשקים שבין אבטחת מידע ובינה מלאכותית, מרצה בתחומי הסייבר והבינה המלאכותית לתארים מתקדמים באוניברסיטת רייכמן ות"א, ומנחה אקדמי של סטודנטים לתארים מתקדמים. ד"ר בירמן מנהל ומקים את מרכז הסייבר של Lenovo בישראל. לפני כן, ניהל את מעבדות מחקר הסייבר של Huawei בישראל. בנוסף, משמש כמבקר אקדמי של IEEE ו- Elsevier ומנהל את בית הספר לסייבר של Google Reichman Tech School. ד"ר בירמן צבר את ניסיונו המקצועי בעבודה במסגרות עסקיות וביטחוניות ואת הכשרתו האקדמית באוניברסיטת בן גוריון ואוניברסיטת ת"א.

עוזר הוראה ומוביל טכנולוגי:

יותם לויט, חוקר אבטחת סייבר וחבר צוות הקמה במעבדת מחקר לאבטחת סייבר של Lenovo Research. בוגר יחידת המודיעין 8200 ובעל ניסיון במחקר תעשייתי. כיום מתמחה במחקר פתרונות סייבר מבוססי בינה מלאכותית.

ניהול סיכוני סייבר

תכנית המפגשים

1	8.9.2026 17:00-21:00	מבוא לאבטחת סייבר למנהלים וסייבר בעולם הפיזי
2	15.9.2026 17:00-21:00	ניהול מדיניות ורגולציות בתחום הסייבר (Governance & Compliance) ותפקיד ה-CSO
3	6.10.2026 17:00-21:00	האחריות המשפטית של ההנהלה בתחום הסייבר וטכנולוגיות תומכות הליכים משפטיים
4	13.10.2026 17:00-21:00	הגנת נתונים, פרטיות מידע וניהול משברי סייבר
5	20.10.2026 17:00-21:00	הערכת סיכונים והטמעת תרבות סייבר ארגונית
6	*28.10.2026 17:00-21:00	הערכת סיכונים והטמעת תרבות סייבר ארגונית
7	3.11.2026 17:00-21:00	ניהול סיכונים וביטוחי סייבר RISKS
8	10.11.2026 17:00-21:00	סימולציה מסכמת

* המפגשים בימי שלישי במתכונת פרונטלית בקמפוס אוניברסיטת רייכמן, למעט מפגש מספר 6 שיהיה מפגש חוץ ויערך ביום רביעי

** FORE לימודי חוץ והכשרת מנהלים, אוניברסיטת רייכמן שומר לעצמו את הזכות לערוך שינויים קלים בתכנית

למסיימי הקורס תוענק תעודה מטעם FORE לימודי חוץ והכשרת מנהלים, אוניברסיטת רייכמן
בעבור 42 שעות אקדמיות. קבלת התעודה מותנית בנוכחות של 80%

ניהול סיכוני סייבר

פירוט המפגשים

1 יום ג' 08.09.2026

מבוא לאבטחת סייבר למנהלים וסייבר בעולם הפיזי

המפגש הפותח של הקורס יעניק למנהלים סקירה רחבה ומעמיקה על עולם הסייבר – האיומים, ההגנות, והאחריות הניהולית הנגזרת מהם.
נבין כיצד מתקפות סייבר משפיעות על מגזרים שונים, אילו תחומי הגנה קיימים, ומה תפקידו הקריטי של הדרג הניהולי ביצירת חוסן ארגוני.
נלמד מהמובילים בתעשייה, נחשף לממשקי המדינה והמערכת הלאומית להגנת הסייבר, ונגלה זירות חדשות לאיומים.
בחלקו האחרון של המפגש תתקיים **הדגמה חיה של רובוט דמוי אדם** במסגרת הרצאה בנושא סייבר בממד הפיזי, שתועבר על ידי ראש תחום אבטחת רובוטיקה ב- Lenovoישראל, שתמחיש כיצד סייבר יוצא מגבולות המסך ומשפיע על העולם הפיזי סביבנו.

ד"ר יוני בירמן; בן חקלאי, סמנכ"ל טכנולוגיות לאומיות, Microsoft Israel; **דדי גרטלר**, מומחה להגנת סייבר, לשעבר ראש אגף בכיר לחדשנות ושת"פ טכנולוגי במערך הסייבר הלאומי, משרד ראש הממשלה;
איתמר אלקיים, ראש תחום אבטחת רובוטיקה ובינה מלאכותית פיזית, Lenovo ישראל

2 יום ג' 15.09.2026

ניהול מדיניות ורגולציות בתחום הסייבר (Governance & Compliance) ותפקיד ה -CSO

המפגש יציג בפני המשתתפים את עולם המדיניות, הרגולציה והציות בסייבר - מרכיב מרכזי בניהול אסטרטגי של סיכוני סייבר בארגון. נבחן כיצד רגולציות גלובליות כגון GDPR, NIS2, SEC מעצבות את פעולת הארגון, נלמד מה ההבדל בין ציות לניהול סיכונים, וכיצד ניתן להטמיע מדיניות סייבר מותאמת לארגון.
נלמד מהו תפקידו של ה- CISO ומה אחריותו בתכנון והפעלה של מערך הסייבר הארגוני, ונכיר טכנולוגיות מתקדמות לניהול מדיניות וציות (GRC) כולל הדגמות חיות מחברה חדשנית בתחום.

דרור חבלין, מנהל אבטחת מידע (CISO), מכבי שירותי בריאות

3 יום ג' 06.10.2026

האחריות המשפטית של ההנהלה בתחום הסייבר וטכנולוגיות תומכות הליכים משפטיים

המפגש יציג בפני המשתתפים את עולם המדיניות, הרגולציה והציות בסייבר - מרכיב מרכזי בניהול אסטרטגי של סיכוני סייבר בארגון. נבחן כיצד רגולציות גלובליות כגון GDPR, NIS2, SEC מעצבות את פעולת הארגון, נלמד מה ההבדל בין ציות לניהול סיכונים, וכיצד ניתן להטמיע מדיניות סייבר מותאמת לארגון.
נלמד מהו תפקידו של ה- CISO ומה אחריותו בתכנון והפעלה של מערך הסייבר הארגוני, ונכיר טכנולוגיות מתקדמות לניהול מדיניות וציות (GRC) כולל הדגמות חיות מחברה חדשנית בתחום.

ד"ר יובל ריינפלד, בית ספר הארי רדזינר למשפטים, אוניברסיטת רייכמן יו"ר (משותף) ועדת בינה מלאכותית בלשכת עוה"ד, וחבר בפורום המומחים הלאומי לבינה מלאכותית ; **ד"ר מתן גוטמן**, מייסד חברת CRT יועץ לארגונים וחבר המועצה להגנת הפרטיות, משרד המשפטים; **ניר אדלר**, Director of Incident Response ,Sygnia

ניהול סיכוני סייבר

פירוט המפגשים

4 יום ג' 13.10.2026

הגנת נתונים, פרטיות מידע וניהול משברי סייבר

המפגש יתרכז בשני נושאים, הראשון, הגנת הנתונים ופרטיות המידע, והשני, בעתיד איומי הסייבר, בדגש על השפעת הבינה המלאכותית. בחלקו הראשון נעמיק באחריות המשפטית של הנהלה על פרטיות ואבטחת מידע, נלמד על רגולציות מקומיות וגלובליות, ונחשף לפתרונות טכנולוגיים חדשניים שמסייעים לארגונים להתמודד עם אתגרי דלף מידע והגנה על נכסי מידע רגישים.
בחלקו השני של השיעור נדון וניחשף לוקטורי ההתקפה ויכולות ההגנה החדשים והמתפתחים בעולם הסייבר, בדגש על כיצד הבינה המלאכותית משפיעה עליהן.

עו"ד עלי קלדרון, ממונה הגנת הפרטיות (DPO) מגדל חברה; **נועם פורר**, סמנכ"ל אסטרטגיה ודיגיטל, בן חורין אלכסנדרוביץ, אסטרטגיה תקשורת וניהול משברים; **אל"מ (מיל') דורון הדר,** מומחה לניהול משברים ושותף מייסד חברת קריטיקל אימפקט

5 יום ג' 20.10.2026

מפגש חוץ – ביקור בחברת אבטחת המידע Palo Alto Networks

פרטי המפגש יפורטו בהמשך

6 יום ג' 20.10.2026

ניהול משברי סייבר והטמעת תרבות סייבר ארגונית

המפגש השישי יעסוק בהערכת סיכונים והטמעת תרבות סייבר, תוך חיבור ישיר למציאות בשטח.
נארח מומחה המגיע מחזית העשייה, שיציג אירועי אמת ואיומים עדכניים - מזווית הראייה הארגונית ועד לזירה הלאומית.
ההרצאה תמחיש כיצד הבנת האיומים בפועל מהווה את הבסיס הקריטי לניהול סיכונים חכם ולבניית תרבות סייבר ארגונית.

דדי גרטלר, מומחה להגנת סייבר, לשעבר ראש אגף בכיר לחדשנות ושת"פ טכנולוגי במערך הסייבר הלאומי, משרד ראש הממשלה

ניהול סיכוני סייבר

פירוט המפגשים

7 יום ג' 03.11.2026

ניהול סיכונים וביטוחי סייבר RISKS

המפגש החמישי יתמקד בתהליכי ניהול סיכונים ארגוניים ובממשק שבין סייבר לעולם הביטוח. בחלקו הראשון נלמד על מתודולוגיות מובילות להערכת וניהול סיכוני סייבר, תוך סקירה של כלים טכנולוגיים לזיהוי, תיעדוף וטיפול באיומים. המשתתפים יקבלו כלים יישומיים להובלת תהליך קבלת החלטות אסטרטגי תחת סיכון.
החלק השני של המפגש יעסוק בעולם ביטוחי הסייבר - כיצד נבנית פוליסה, איך מתבצעת הערכת סיכונים מצד המבטח, ומהי אחריות ההנהלה בהיערכות מול תרחישי משבר מנקודת מבט ביטוחית.

ניר סלינס, מנהל אבטחת המידע הראשי (CISO), בנק הפועלים ; **דמי בן-ארי,** מייסד משותף ומנהל טכנולוגי (CTO), Panorays ; **שי סימקין,** ראש תחום ביטוחי הסייבר, קבוצת Howden העולמית

8 יום ג' 10.11.2026

סימולציה מסכמת

המפגש השמיני הינו מפגש הסיכום של הקורס, בו נתמקד בתהליכי קבלת ההחלטות וניהול אירועי סייבר ברמת מקבלי ההחלטות והמנהלים. במהלך המפגש נבצע סימולציה של אירוע סייבר תוך חלוקה לקבוצות עם אוריינטציות ומטרות שונות, על מנת לפתח ולחוות את תרחישי קבלת ההחלטות וניהול הסיכונים מזוויות שונות.
באמצעות תרגיל ה־ Tabletop, מנהלים מחברת Cyberpro יפעילו סימולציה אסטרטגית המדמה תרחיש משבר אמיתי בארגון, המאפשר למשתתפים להתנסות בקבלת החלטות בזמן אמת, תחת לחץ ובתנאי אי-ודאות.
במהלך התרגיל, הצוותים ידרשו לנתח את האירוע, להבין את ההשלכות העסקיות והטכנולוגיות, לתאם בין בעלי תפקידים שונים ולהוביל את הארגון להתאוששות מיטבית. התוצאה היא שיפור משמעותי ברמת המוכנות הארגונית, חיזוק תהליכי התגובה לאירועי סייבר, והעמקת שיתוף הפעולה בין גורמי ההנהלה, ה- IT והאבטחה, כך שהארגון יוכל להתמודד בצורה אפקטיבית ומהירה יותר עם כל משבר עתידי.

חברת Cyberpro