אוניברסיטת רייכמן
FORE לימודי חוץ והכשרת מנהלים

קורס ניהול סיכוני סייבר 2025

ניהול אקדמי: ד"ר יוני בירמן

תאריך פתיחה: 7.09.25
8 מפגשים 17:00-21:00

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

תאריכי המפגשים:
7.9.25 • 14.9.25 • 21.9.25 • 28.9.25 • 5.10.25 • 19.10.25 • 26.10.25 • 21.11.25

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 2025 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. יעניק 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).
- 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 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.

ניהול סיכוני סייבר

תכנית המפגשים

1	7.9.2025 17:00-21:00	מבוא לאבטחת סייבר למנהלים
2	14.9.2025 17:00-21:00	האחריות המשפטית של ההנהלה בתחום הסייבר וטכנולוגיות תומכות הליכים משפטיים
3	21.9.2025 17:00-21:00	ניהול מדיניות ורגולציות בתחום הסייבר (Governance & Compliance) ותפקיד ה-CSO
4	28.9.2025 17:00-21:00	הגנת נתונים, פרטיות מידע ועתיד האיומים בסייבר וב-AI
5	5.10.2025 17:00-21:00	ניהול סיכונים וביטוחי סייבר
6	19.10.2025 17:00-21:00	ניהול משברי סייבר והטמעת תרבות ומודעות סייבר ארגונית
7	* 26.10.2025 17:00-21:00	בנייה והפעלה של מערך הסייבר הארגוני ופאנל מומחים לסיכום ההכשרה מטעם חברת Check Point *המפגש יתקיים במשרדי חברת Check Point
8	2.11.2025 17:00-21:00	סימולציה מסכמת

* המפגשים במתכונת פרונטלית בקמפוס אוניברסיטת רייכמן, למעט מפגש מספר 7 שיערך במשרדי חברת Check Point
** 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%

אוניברסיטת רייכמן
FORE לימודי חוץ והכשרת מנהלים

ניהול סיכוני סייבר

פירוט המפגשים

1 יום א' 7.9.2025

מבוא לאבטחת סייבר למנהלים

המפגש הפותח של הקורס ייתן 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 – כמו המדיה החברתית – מזווית שלא הכרתם.

ד"ר יוני בירמן, בן חקלאי, סמנכ"ל טכנולוגיות לאומיות Microsoft Israel ; **דדי גרטלר,** ראש אגף בכיר לחדשנות ושת"פ טכנולוגי, מערך הסייבר הלאומי; **רון אזוגי,** מייסד משותף ו-CTO, Spikerz

2 יום א' 14.9.2025

האחריות המשפטית של ההנהלה בתחום הסייבר וטכנולוגיות תומכות הליכים משפטיים

במפגש זה נצלול להיבטים המשפטיים הקריטיים שכל מנהל חייב להכיר בעידן הדיגיטלי. נלמד מהי אחריותו המשפטית של הדרג הבכיר במקרה של מתקפת סייבר – מההיערכות המקדימה ועד ההתמודדות עם ההשלכות.
נבין כיצד לפעול במצבי רגולציה מעורפלת, ואיך ניתן לנהל סיכונים משפטיים וטכנולוגיים בעולם שבו החוקים משתנים לאט מהאיומים.
נסיים בהיכרות עם טכנולוגיות מתקדמות כמו eDiscovery, -iDigital Forensics כולל הדגמה של כלי חקירה דיגיטליים ומקרי בוחן מעשיים.

מרצים: פרופ' מורן אופיר, חברת סגל באוניברסיטת חיפה ומרצה באוניברסיטת רייכמן; **ד"ר מתן גוטמן,** מייסד חברת CRT יועץ לארגונים וחבר המועצה להגנת הפרטיות, משרד המשפטים; **אורי פורג,** מנהל מערך פתרונות תגובה לאירועי סייבר, Sygnia

3 יום א' 21.9.2025

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.

מרצים: גידי פרקש, סמנכ"ל אבטחת מידע ותפעול Pipl, **ניר סלניס,** מנהל מחלקת הגנת הסייבר (CISO), חטיבה טכנולוגית, מכבי שירותי בריאות ; **יאיר קוזניצוב,** מייסד משותף ומנכ"ל, Anecdotes

ניהול סיכוני סייבר

פירוט המפגשים

4 יום א' 28.9.2025

הגנת נתונים, פרטיות מידע ועתיד האיומים בסייבר וב-AI

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.

מרצים: עו"ד עלי קלדרון, ממונה הגנת הפרטיות (DPO) מגדל חברה לביטוח; **נמרוד וקס,** מייסד שותף ו- CPO BigID; **דורית דור,** מייסדת שותפה, Qbeat Ventures ויועצת עמיתה, Check Point

5 יום א' 5.10.2025

ניהול סיכונים וביטוחי סייבר

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.

מרצים: יוני אפרתי, מנהל אבטחת מידע (CISO) בנק הפועלים; **דמי בן-ארי,** מייסד משותף ומנהל טכנולוגי Panorays (CTO); **שי סימקין,** ראש תחום ביטוחי הסייבר, קבוצת Howden Broking

6 יום א' 19.10.2025

ניהול משברי סייבר והטמעת תרבות ומודעות סייבר ארגונית

המפגש השישי יעסוק בשני היבטים שתלויים כמעט אך ורק בדרג מקבלי ההחלטות ובאופן שבו הם בוחרים לנהל את תפיסת ההגנה בסייבר הארגונית – כיצד מייצרים תרבות ומודעות סייבר ארגונית בריאה וכיצד נערכים ומתמודדים במידה וחווינו משבר סייבר.
בחלקו הראשון של השיעור נכיר את עולם ניהול משברי סייבר משלל היבטיו – איך מזהים, מגיבים ומנהלים אירוע סייבר בזמן אמת. נלמד כיצד מתבצע משא ומתן עם תוקפים, נבין את מרכיבי קבלת ההחלטות, כלים לניהול ותגובה לאירועים קריטיים ו נלמד על ניהול משברי סייבר מנקודת מבט תקשורתית וציבורית
בחלקו השני של השיעור נעסוק בבניית תרבות ארגונית בתחום הסייבר והכלים הטכנולוגיים העומדים לרשותנו להעלאת המודעות ושיפור תרבות הסייבר הארגונית.

מרצים: עומר בז'רנו, ראש תחום הצלחת לקוח (Head of Customer Success & Services), Cytactic ; **ד"ר ארי אחיעז,** מרצה, חוקר ויועץ בתחומי המימון ותקשורת במשברי סייבר, אוניברסיטת רייכמן ;**מייק פולצ'ק,** שותף מייסד ומנכ"ל Cyberead ; **אסף גולדברג,** סגן נשיא למכירות, אירופה, אפריקה והמזה"ת, Cybeready

ניהול סיכוני סייבר

פירוט המפגשים

7 יום א' 26.10.2025

בנייה והפעלה של מערך הסייבר הארגוני ופאנל מומחים לסיכום ההכשרה מטעם חברת Check Point

***המפגש ייערך במשרדי Check Point**

המפגש השביעי יעסוק במערך הסייבר הארגוני אשר אמון על היערכות, תפעול ותגובה לאירועי התקפה בסייבר ויכלול פאנל Q&A של מומחים בכירים מטעם חברת Check Point בו נוכל לקבל תשובות על כל הנושאים שנלמדו במהלך ההכשרה מנקודת מבט מקיפה.
בחלקו הראשון של השיעור נכיר את מגוון בעלי התפקידים אשר אמונים על מערך הסייבר הארגוני, את המערכות והכלים בהם משתמשים, תהליכי קבלת החלטות והממשקים להנהלה ואילו חלופות עומדות בפני מנהלים כאשר נדרשים או מעוניינים להקים מערך כזה.
בחלקו השני של השיעור, שיציין את נקודות השלמת הלימודים/הרצאות, נקיים פאנל Q&A יחד עם מומחים בכירים של חברת Check Point בו משתתפי ההכשרה יוכלו לשאול וללמוד ממוחי הסייבר המובילים במדינה ובעולם.

8 יום א' 02.11.2025

סימולציה מסכמת

המפגש השמיני הינו מפגש הסיכום של הקורס, בו נתמקד בתהליכי קבלת ההחלטות וניהול אירועי סייבר ברמת מקבלי ההחלטות והמנהלים. במהלך השיעור, נבצע סימולציה של אירוע סייבר תוך חלוקה לקבוצות עם אוריינטציות ומטרות שונות, על מנת לפתח ולחוות את תרחישי קבלת ההחלטות וניהול הסיכונים מזוויות שונות.

מרצים: הסימולציה תועבר על ידי מנהלים בכירים מחברת Cytactic