

### תיבה א'-1- מבחן קיצון אחיד למערכת הבנקאות שמבוסס על תרחיש סייבר, 2019

- התקפות הסייבר נגד ארגונים בעולם ובהם גם התקפות נגד המגזר הפיננסי, עלו בשנים האחרונות בכמותן ובתחכומן. מגמה זו מעלה את החשש מפני התקפת סייבר בישראל בכלל ובמערכת הבנקאות בפרט.
- לסיכון הסייבר מאפיינים ייחודיים ובהם העובדה שהתקפות סייבר הן זדוניות ולעיתים מכוונות, ממוקדות, מתוחכמות ומבוצעות לאחר תכנון ארוך טווח. בשל מאפיינים אלה, ההשלכות של התקפת סייבר עלולות להיות בלתי צפויות ולכן יש גם קושי בהערכת עוצמת הפגיעה הצפויה מאירוע כזה.
- במטרה לחזק את ניהול סיכון הסייבר במערכת הבנקאות ובמטרה לשפר את הבנת הפיקוח על הבנקים בתחום סיכון הסייבר והשלכותיו על יציבות הבנקים, הפיקוח על הבנקים ערך השנה מבחן קיצון אחיד למערכת הבנקאות, שמבוסס על תרחיש סייבר. תרחיש קיצון במתכונת זו הוא ראשון מסוגו בפיקוח על הבנקים וככל הידוע לנו - בכלל גופי פיקוח הפיננסיים בעולם. חשוב לציין שתרחיש הקיצון אינו תחזית, אלא תרחיש קיצוני משוער, שנועד לבחון את התמודדותו של הבנק עם סיכון מעין זה.
- בסיס המבחן הוא תרחיש אירוע סייבר חמור, שבמסגרתו שובשו נתוני העו"ש והפיקדונות של כלל הלקוחות הפרטיים בבנק. אירוע זה מוביל להשפעות טכנולוגיות ולהשפעות פיננסיות על הבנק ועל לקוחותיו ולכן, מכסה, בין היתר, את תחום סיכון הסייבר, הסיכון התפעולי, סיכון הציות, הסיכון המשפטי וסיכון המוניטין ואת הסינרגיה בין הסיכונים הללו ומאתגר גם את ניהול המשכיות העסקית של הבנק.
- מבחן הקיצון בתרחיש זה איפשר לבחון את מוקדי הסיכון שעולים מהתממשות של אירוע סייבר חמור ואת השפעותיו הישירות והעקיפות על הפעילות הבנקאית ועל ההתמודדות מולו, לרבות פעילות הבנק מול לקוחותיו, ההשפעות על מערכות המידע של הבנק וההשלכות הפיננסיות כתוצאה מהתרחיש, הן בטווח הקצר והן בטווח הארוך.
- מבחן זה סייע לבנקים לאתר את הפערים שעליהם לצמצם לשם התמודדות עם תרחיש בהיקף כזה, והוא צפוי לסייע בבניית תכניות מגירה שונות למקרה של אירועים עתידיים מסוג זה ובחיזוק ערוץ התקשורת בין היחידות השונות בבנק לשם התנהלות במקרה של אירוע כזה. תרחיש זה תרם גם לחיזוק הידע שקיים בפיקוח על הבנקים ובמערכת הבנקאות ביחס לאירוע מעין זה ולהשלכות שנלוות לו, לרבות לאפשרות של פגיעה ביציבות הבנק, והוא יהווה כלי עזר להסקת מסקנות פיקוחיות וקביעת פעילויות המשך בנושא.
- משבר הקורונה העצים סיכונים שונים, לרבות את סיכון הסייבר, ובכך מחדד את חשיבות היערכותה השוטפת של המערכת הבנקאית להתמודדות עם הסיכונים הנשקפים למערכת הבנקאית, בין היתר באמצעות קיומם של מבחני קיצון השונים, לרבות מבוססי תרחיש סייבר.

#### רקע

הפיקוח על הבנקים עורך מבחני קיצון אחידים למערכת הבנקאות מאז שנת 2012, במטרה לתרום להבנת מוקדי הסיכון, שמערכת הבנקאות וכל אחד מהבנקים חשופים להם. השנה הוחלט שמבחן הקיצון האחיד יבחן את מוקדי הסיכון שעולים נוכח התממשות אירוע קיצון בתחום הסייבר, שבמהותו מגלם השפעות נוספות, מעבר לנזק ישיר של אירוע סייבר חמור. תהליך זה צפוי לתרום לחיזוק ולשיפור תהליכי ניהול סיכון הסייבר במערכת הבנקאות בישראל ולסייע לחיזוק הידע שקיים בפיקוח על הבנקים ובמערכת הבנקאות ביחס לאירוע מעין זה ולהשלכות שנלוות לו. מבחן זה הוא המשך לפעילות קודמת של הפיקוח על הבנקים מול מערכת הבנקאות בשנים 2017-2018 בנושא תרחישי קיצון סייבר (במסגרתה הפיקוח על הבנקים בחן את מבחני הקיצון הפנימיים המבוססים על אירוע סייבר שביצעו הבנקים) כשהשנה הוחלט להגדיר תרחיש אחיד לכל המערכת.

### סיכון הסייבר במערכת הבנקאות

התקפות הסייבר נגד ארגונים בעולם ובהן גם התקפות נגד המגזר הפיננסי<sup>76</sup>, עלו בשנים האחרונות בכמותן ובתחכומן. מגמה זו מעלה את החשש מפני אירוע סייבר מהותי בישראל בכלל ובמערכת הבנקאות בפרט. לפי סקרי סיכונים שביצע הפיקוח על הבנקים בקרב בכירי מערכת הבנקאות בפברואר 2019 ובפברואר 2020, עולה שהסיכון שמטריד ביותר הוא סיכון הסייבר<sup>77</sup> ושרובם המכריע של בכירי המערכת רואים בו את אחד משלושת הסיכונים המשמעותיים ביותר שעומדים מאחורי מערכת הבנקאות.

לסיכון הסייבר מאפיינים שונים משאר הסיכונים שניצבים בפני מערכת הבנקאות. בשונה, לדוגמה, מזעזוע פיננסי, שנובע מזעזוע חיצוני (שהתגובה לו בשווקים יחד עם אפקט ההדבקה, יכולה ליצור נזק רב), התקפת סייבר היא יזומה ולעיתים מכוונת, ממוקדת, מתוחכמת ומבוצעת לאחר תכנון ארוך טווח<sup>78</sup>. במתקפות מתוחכמות כאלו, התוקפים חוזרים למערכות שבועות ואף חודשים מראש, כדי למפות אותן, במטרה להבין מהי הדרך המיטבית לשיבוש המערכות. התוקף נדרש אמנם למשאבים רבים ולתכנון מוקדם כדי להוציא לפועל את ההתקפה, אך ההתקפה תבוצע בתזמון לפי בחירתו של התוקף ובאופן שיקשה על עצם זיהוי ההתקפה. כך, כשתתגלה ההתקפה, ייתכן מאד שיוסב כבר נזק משמעותי לגורם הנתקף. הסיכוי להצלחה של התקפה כזו הוא גבוה וההתקפה תהיה בעלת השפעה גבוהה. בנוסף, מרחב הסייבר הוא מורכב מאוד: המערכות עצמן מרושתות, מחוברות זו לזו ותלויות זו בזו. לכן, שיבוש במערכת אחת יכול לגרור אחריו באופן בלתי צפוי שיבושים באזור אחר, כך שלא ברור כיצד שיבוש במערכת אחת יכול לדרדר את שאר המערכות. הדבר שונה מסיכונים פיננסיים, שבהם ההשפעות השונות על התחומים השונים והקשרים בין התחומים השונים, נחקרו ונאמדו באמצעות מודלים שנשענים על אירועי עבר. הדבר מביא לכך שההבנה של ההשפעות הפיננסיות על מערכת הבנקאות ברורות יותר ביחס להשפעותיו של מתקפת סייבר וכך גם הכלים שבעזרתם ניתן להקטין את הסיכונים הללו. (Healy et al., 2018).

בהינתן התממשותו של אירוע סייבר במערכת הבנקאות, ההשלכות עלולות להיות משמעותיות, הן עבור הבנק הבודד והן עבור היציבות הפיננסית כולה. אחד מהחששות המרכזיים, עם התממשותו של אירוע סייבר משמעותי בבנק, הוא התרחשותו של Cyber Run ("ריצה אל הבנק" על רקע אירוע סייבר), קרי, משיכת פיקדונות מסיבית מצד המפקידים בבנק, מחשש לפגיעה בהם, לאור התקפת הסייבר וכן בשל פגיעה משמעותית במוניטין הבנק. משיכה משמעותית של פיקדונות עלולה לגרום לפגיעה בנזילות הבנק וביכולתו לעמוד בהתחייבויותיו לתשלומים בזמן. בנוסף, משבר נזילות בבנק מסוים, עלול לגרור אחריו השלכות משמעותיות על כלל המשק, גם זמן רב לאחר שהבנק חזר לתפקוד והנגישות לפיקדונות חזרה וזה משום שהעיכוב בתשלומים, יחד עם חוסר הוודאות, משליכים גם על המוסדות הפיננסיים האחרים ובפרט כשהם לא מקבלים את התשלומים שהם היו אמורים לקבל (Duffie and Younger, 2019).

<sup>76</sup> לסקירת אירועי סייבר שהתרחשו במגזר הפיננסי במדינות שונות בשנים 2016-2018, ראו תיבה א'-3 בסקירת מערכת הבנקאות לשנת 2018.

<sup>77</sup> להרחבה, ראו פרק הסיכונים בסקירת מערכת הבנקאות לשנת 2018 ופרק הסיכונים בסקירה זו

<sup>78</sup> התקפות אלה מכונות APT - Advanced Persistent Threat ומהוות את אחד הסיכונים המרכזיים בתחום הסייבר. מדובר בתוקפים מיומנים ומתקדמים, שממוקדים בתקיפה מכוונת של ארגון מסוים.

נוכח סיכונים אלה, מבטאים רגולטורים רבים בעולם כמו גם הפיקוח על הבנקים<sup>79</sup>, בין היתר, באמצעות רגולציה, את חשיבות ניהול סיכון הסייבר. החוקרים Kashyap ו-Wetherilt מהבנק המרכזי בבריטניה, ציינו במאמם "Some Principles for Regulating Cyber Risk" כמה עקרונות רגולטוריים מרכזיים, לפיהם יש לפעול כדי לחזק את אופן ניהול סיכון הסייבר בכלל המערכת הפיננסית, לרבות בבנקים ובהם:

- לדרוש שהחברות יפעלו תחת ההנחה שמניעה מוחלטת של התקפה מוצלחת עם השפעה גבוהה היא בלתי אפשרית<sup>80</sup>. כמו כן, מצופה שהחברות ימשיכו לפעול, למרות ההפרעות במערכתיהן. דרישה זו מביאה חברות לאפיין מהן אותם שירותים קריטיים שהם צריכים להצליח להמשיך ולספק במקרה של התקפת סייבר.
- לדרוש שהחברות יתכוננו לפגיעה ארוכת טווח וכלל מערכתית, בדגש על המשאבים שנדרשים להתאוששות ולתגובה לאירוע, שכן, הם עלולים להיות מוגבלים. עקרון זה מעודד את החברות לתכנן את מרחב התרחישים האפשריים ולהתחשב גם בהשלכות שקיימות גם מחוץ לכותלי החברה שלהם.
- לשאוף לדו-שיח דו-כיווני בין חברות ומפקחים, כחלק מגישה רחבה יותר לשיתוף פעולה בתחום, שיאפשר ללמוד ולפתח כלים להערכה וניהול של סיכונים הסייבר.

כמו כן, לפי מאמר זה, מציפים הרגולטורים השונים בעולם את הצורך בקיום תרחישי קיצון בתחום הסייבר. בפועל, הבנקים מבצעים אמנם תרגילי סייבר ותרחישי קיצון פנימיים בתחום, אך עד כה לא מצאנו בבדיקתנו בנק מרכזי או רגולטור, שערך מבחן קיצון אחיד למערכת הבנקאות המבוסס על תרחיש סייבר. יתכן שהסיבה לכך נובעת, בין היתר, מהעובדה שיש קושי לערוך שימוש במודלים, כדי לאמוד את סיכון הסייבר זה, כאמור, בשונה מתרחיש קיצון מקרו-כלכלי.

#### מבחן קיצון מבוסס תרחיש סייבר

מבחן הקיצון שקיים הפיקוח על הבנקים במהלך 2019, נועד לבחון את אופן התמודדותו של בנק עם התקפת סייבר משמעותית וחמורה ועם השלכותיה בטווח הזמן המיידי ובטווח הזמן הארוך. בסיס המבחן הוא תרחיש אירוע סייבר חמור אך סביר, שעיקרו אירוע שיבוש נתונים, המוביל להשפעות טכנולוגיות, תפעוליות ולהשפעות פיננסיות על הבנק ועל לקוחותיו. לכן הבנקים נדרשו לבחון את כלל השפעות ההתקפה על פעילות הבנק, הן הישירות והן העקיפות, לרבות פעילות הלקוחות, ההשפעה על מערכות המידע של הבנק וההשלכות הפיננסיות. בשונה מתרחישים מקרו-כלכליים, במבחן קיצון זה נדרש כל בנק לנתח את התרחיש תחת ההנחה שרק הוא עצמו נפגע מהתרחיש ושאר מערכת הבנקאות לא נפגעה, במטרה להעצים את הפגיעה האפשרית בבנק הבודד (ולבחון את התמודדותו עם פגיעה במוניטין הבנק ועם ההשלכות שנלוות לכך בפרט). הבנק נדרש להניח הנחות בדבר פעולות וצעדים שהנהלה הייתה נוקטת בעת התממשות תרחיש זה ולפרטן בניתוח התרחיש. חשוב לציין שתרחיש הקיצון אינו תחזית, אלא תרחיש קיצוני משוער, שנועד לבחון את התמודדותו של הבנק עם סיכון מעין זה.

<sup>79</sup> בין היתר, בהוראת ניהול בנקאי תקין מס' 361 "ניהול הגנת הסייבר" והוראת ניהול בנקאי תקין מס' 363 "ניהול סיכונים סייבר בשרשרת אספקה".

<sup>80</sup> כך גם בסעיף 26 ו' בהוראת ניהול בנקאי תקין מס' 361 "ניהול הגנת הסייבר".

הבנקים נדרשו לנתח בנפרד את השלכות התקפת הסייבר הן בטווח המיידי - מרגע גילוי ההתקפה ועד לזיהוי מקור ואופן ההתקפה<sup>81</sup>; הן בטווח הקצר-בינוני - משלב הבנת הפגיעה ועד תום ההתאוששות הטכנולוגית; והן בטווח הארוך - משלב ההתאוששות הטכנולוגית ועד לסיום התקופה שבה יחוו את כלל השלכות ההתקפה, לרבות היבטי מוניטין, היבטים משפטיים וכו"ב. שכן, כפי שעולה מאירועי סייבר משמעותיים בעולם, ההשלכות הנוספות של התקפות סייבר עלולות להיות ממושכות וההתמודדות עמן נפרסת על פני תקופת זמן ארוכה. הבנקים נדרשו לפרט בהרחבה לגבי פעולות שנקטו לכל אורך התרחיש האמור, לרבות החלטות ההנהלה שנקטו בכל שלב, השלכות ההתקפה וההתמודדות עימה בכלל התחומים - טכנולוגיה וסייבר, פעילות הבנק מול לקוחותיו וההשלכות הפיננסיות.

### מטרות התרחיש

לביצוע תרחיש הקיצון יש כמה מטרות. בעבור הבנקים, מצופה שתהליך זה יתרום לחיזוק ולשיפור תהליכי ניהול סיכון הסייבר והשלכותיו. תרחיש זה מכסה את תחום סיכון הסייבר, הסיכון התפעולי, סיכון הציות, הסיכון המשפטי וסיכון המוניטין וכן מאתגר את ניהול ההמשכיות העסקית של הבנק. לכן, במסגרת המענה לתרחיש, נדרשו כלל החטיבות השונות בבנקים לבחון את השפעת התרחיש בגזרתן ולפעול בשיתוף פעולה, כדי לגבש את המענה לתרחיש<sup>82</sup>. עבודה זו נועדה לתרום להבנת הפערים שמצויים בבנק להתמודדות עם תרחיש מעין זה, לבניית תכניות מגירה שונות למקרה של אירועים עתידיים ולחיזוק ערוץ התקשורת בין היחידות השונות לשם היתכנות ההתנהלות במקרה של אירוע כזה.

מבחינה פיקוחית, ניתוח התרחיש מאפשר לזהות אזורי פגיעות ומוקדי סיכון שהבנק עלול להיות חשוף להם בעת התממשותו של אירוע סייבר חמור. בנוסף לעמידותו הפיננסית של הבנק לאירוע מעין זה, נבחנו גם השפעות התרחיש על רמת השירות שהבנק יכול לספק ללקוחותיו, הבקורות שקיימות לזיהוי התקפת סייבר, אופן התאוששותו של הבנק בהיבטים טכנולוגיים ותפעוליים וכן צעדי ההנהלה והפעולות שבהן הבנק נקט, לכאורה, כדי להתמודד עם האתגרים שעלו במבחן זה. תשובותיהם של הבנקים יסייעו בהערכת נאותות היבטים אלה בתהליך ניהול הסיכון וישתלבו בתהליכי ההערכה הפיקוחיים (SREP). נוסף על כל אלה, יתרום תרחיש זה לחיזוק הידע שקיים בפיקוח על הבנקים ביחס לאירוע סייבר מהותי וההשלכות שנלוות לו, באמצעות קבלת מידע כמותי ואיכותי בתחומים שונים, לרבות אפשרות הפגיעה ביציבות הבנק נוכח אירוע מעין זה.

### סיפור הרקע בבסיס מבחן הקיצון

חברה שמהווה חלק משרשרת האספקה של הבנק חווה התקפת סייבר על ידי גורם זדוני במועד לא ידוע וללא ידיעתה. דבר זה מאפשר לגורם הזדוני לפנות בהמשך באופן שוטף לבנק, תוך התחזות לאותה חברה.

<sup>81</sup> במטרה להעצים את פגיעת התרחיש, הוגדר אורך תקופה כזה לבנקים, במנותק מיכולותיו הטכנולוגיות של הבנק לאתר את מקור ואופן ההתקפה. מטרת הגדרה זו היא לאתגר את ההמשכיות העסקית של הבנקים בתקופה של אי-ודאות עסקית וטכנולוגית.

<sup>82</sup> ראו גם חוזר ח-06-2457 (ניהול הגנת הסייבר) סע' 2 – "פרסום הוראה מיוחדת לנושא ניהול הגנת הסייבר כאמור, בא להדגיש את גישת הפיקוח על הבנקים שהתמודדות עם סיכונים הסייבר מהווה נושא חוצה-ארגון, שמחייב מעורבות פעילה של הדרגים הבכירים בתאגיד הבנקאי. על אף שסיכונים הסייבר נובעים משימוש בטכנולוגיות, הם אינם מהווים סוגיה טכנולוגית גרידא, אלא גם סוגיה עסקית-אסטרטגית".

באחת מפניותיו, הוא מותיר במערכות הבנק פוגען לא מוכר, שעוקף את מנגנוני אבטחת הבנק, מתפתח בחשאי במערכות הבנק ומצליח לייצר פגיעה במערכות הליבה שלו. אותו פוגען גורם, ללא ידיעת הבנק ולקוחותיו, לשיבוש אקראי של נתוני יתרת עו"ש (חובה וזכות) ונתוני יתרת פיקדונות של לקוחות קמעונאים במשך חמישה חודשים, בכלל מערכי הגיבוי של מסדי הנתונים של הבנק. בתום חמישה חודשים, השיבוש מופעל גם בסביבת הייצור - דבר שמשתקף מיידית בכלל ערוצי השירות ללקוח, לרבות ערוצים ישירים ודיגיטלי. שיבוש זה משפיע באופן מידי על פעילות הלקוחות של הבנק בתחומים שונים<sup>83</sup>.

### תוצאות התרחיש

ניתוח מבחן הקיצון הוביל את הבנקים לבצע בחינה של הכלים, התהליכים והמערכות שיש ברשותם לשם התמודדות עם מתקפות סייבר. לביצוע תרחיש זה נדרשה גם, כאמור, מעורבות של כלל החטיבות השונות בבנקים, דבר שחיצק הן את יכולת ניהול הסייבר בכל תחום בפני עצמו והן את ניהול הסיכון, בראייה כלל מערכתית. באמצעות תהליך זה זיהו הבנקים מספר פערים שקיימים בקרבם בתחומים שונים וחלקם כבר ביצעו תהליך הפקת לקחים מעמיק ששולבו בתכניות העבודה עם לוחות זמנים ליישומם.

תשובותיהם של הבנקים סייעו לפיקוח על הבנקים לחזק את הידע שקיים בפיקוח אודות סביבת הבקרות, הארכיטקטורה והגיבויים שקיימים בבנק. התרחיש סייע גם להבנת חשיבותם של תהליכים מסוימים בבנקים לשם תפקוד תקין של מערכות הבנק. תשובות הבנקים איפשרו גם לזהות פערים בין הציפיה הפיקוחית באשר להתנהלות באירוע מעין זה, לבין החלטותיהם של הבנקים בפועל, בין היתר, בהיבטי המשכיות העסקית והיבטי בנק-לקוח ותוך הבנת והפנמת האתגר שבקבלת החלטות בתנאי אי-ודאות שמאפיינים את ההתמודדות של גוף שחוהה התקפת סייבר. תוצאות אלה יהוו כלי עזר להסקת מסקנות פיקוחיות וקביעת פעילויות המשך בנושא, כשבין היתר יישקלו עדכונים אסדרתיים שמטרתם להגדיר נהלים ברורים שלפיהם מצופה מהבנקים לפעול בעת התמודדות עם אירועי המשכיות עסקית בכלל וסייבר בפרט.

### תרחיש הסייבר על רקע משבר הקורונה העולמי

משבר הקורונה הוביל, בין היתר, להישענות גוברת של הציבור על ערוצים ישירים ודיגיטליים לקבלת שירותי בנקאות. יתר על כן, חלק ממי שצורכים את השירותים בערוצים הישירים בימים אלה, הם לקוחות שלא מורגלים לשימוש בהם. משבר הקורונה גם אילץ את מערכת הבנקאות להעלות במהירות את היקפי העבודה מרחוק (הן בכמות העובדים שמתחברים מרחוק והן באופן ההתחברות המרוחקת). המשבר העלה גם את הסבירות שהבנקים ייתקלו במחסור בכוח אדם מיומן שנחוץ לטיפול בתקיפות סייבר (בשל מגבלות התנועה וההתקהלות או בשל תחלואה) שינויים אלה העצימו סיכונים שונים והגבירו את החשיפה של מערכת הבנקאות לסיכונים של מעילות, הונאות, שיבושי מידע, דליפת מידע ותקיפות סייבר בכלל. שינויים אלה רלוונטיים גם לגורמי הרשרת האספקה של מערכת הבנקאות, כך שהתעצמות הסיכונים בקרבם, לרבות סיכון הסייבר, משפיעה גם על הסיכונים שמשקפים למערכת הבנקאות.

זאת ועוד, יש חשש בישראל ובעולם לניצול לרעה של רגישות המשק בימים אלה ושל המעבר לעבודה מרחוק של רבים מהעובדים ולניסיונות רבים יותר של תקיפות סייבר. ואכן, מערך הסייבר הלאומי ציין שמאז הכריז ארגון הבריאות העולמי על מצב חירום בשל התפשטות הקורונה, החלו דיווחים אודות מתקפות סייבר שמנצלות את הבהלה הציבורית ברחבי העולם.

<sup>83</sup> כתוצאה משיבוש נתוני העו"ש, מגוון רחב של פעולות לקוחות יתקלו בקשיים, כדוגמת הוראות לחיוב חשבון, העברות בנקאיות וכיו"ב.

ביצוע מבחן קיצון שמבוסס על תרחיש סייבר הוא כלי אחד מיני רבים שבהם נקט הפיקוח על הבנקים בשנים האחרונות לחיזוק ניהול סיכון הסייבר המתעצם. התפתחויות אלה במשבר הקורונה, שהעצימו את מכלול הסיכונים בכלל ואת סיכון הסייבר בפרט, מחדדים את חשיבות היערכותה השוטפת של מערכת הבנקאות להתמודדות עם הסיכונים שנשקפים לה ובהם גם קיומם של מבחני הקיצון השונים. הפיקוח על הבנקים ימשיך לעקוב ולנטר את מכלול הסיכונים שעימם מתמודדת מערכת הבנקאות, לרבות סיכון הסייבר.

#### רשימת מקורות

Duffie, Darrell, and Younger, Joshua. "Cyber Runs." Hutchins Center on Fiscal & Monetary Policy at Brookings. Working Paper n.51. June 2019.

Healey, Jason, et al. "The Future of Financial Stability and Cyber Risk." The Brookings Institution Cybersecurity Project. October 2018.

Kashyap, Anil K., and Wetherilt, Anne. "Some principles for regulating cyber risk." AEA Papers and Proceedings. Vol. 109. 2019.