

## المخاطر السيبرانية في شركات التأمين التكافلي وسبل إدارتها Cyber risks in Takaful insurance companies and ways to manage them

يحيياوي فطيمة<sup>1</sup>، أستاذ محاضر- ب -، جامعة ابن خلدون – تيارت -، الجزائر

[fatima.yahiaoui@univ-tiaret.dz](mailto:fatima.yahiaoui@univ-tiaret.dz)

تاريخ الاستلام: 2023/09/21 ؛ تاريخ القبول : 2023/11/05

### مستخلص

نهدف من خلال هذه الدراسة إلى تحليل المخاطر السيبرانية التي تتعرض لها كل من شركات التأمين التجاري و شركات التأمين التكافلي، خاصة بعد جائحة كورونا والاتجاه نحو الرقمنة، حيث أن هذا الأمر أدى إلى تزايد شدة هذا النوع من المخاطر الذي تتأثر به شركات التأمين بشكل أكبر من غيرها، وذلك بسبب خصوصيتها واعتمادها الكبير على معلومات وبيانات عملائها مما يجعلها هدفا مميز بالنسبة للمخترقين، كما أن العامل الأساسي المسبب لهذه المخاطر يتمثل في الهندسة البشرية التي يتم التلاعب فيها بالأفراد بسهولة، وقد توصلنا من خلال هذه الدراسة إلى أن كل من شركات التأمين التكافلي والتجاري تتعرض للمخاطر السيبرانية بنفس الطريقة، كما أن إدارة هذه المخاطر يعتمد بالدرجة الأولى على عمل الخبراء الإكتواريين.

الكلمات المفتاحية: الخطر السيبراني، التأمين التكافلي، الخبيرالاكتواري

تصنيفاتJEL: O33، G22

### Abstract :

Through this study, our aim is to analyze the cybersecurity risks faced by both commercial insurance companies and takaful (Islamic insurance) companies, especially in the wake of the COVID-19 pandemic and the growing trend towards digitization. This has led to an escalation in the severity of these risks, impacting insurance companies more significantly due to their uniqueness and heavy reliance on customer information and data, making them attractive targets for cyber attackers. The primary factor underlying these risks lies in social engineering, which can easily manipulate individuals. Our study concludes that both takaful and commercial insurance companies are exposed to cybersecurity risks in a similar manner. Furthermore, the management of these risks primarily relies on the work of Actuaries.

**Keywords: cyber risk, Takaful insurance, Actuaries**

Jel Classification Codes :O33 , G22

## مقدمة

"إن شركات التأمين ليست كباقي الشركات فهي لا تسعى للاستفادة من التكنولوجيا، لإن وجودها مرتبط أساس بها". وذلك راجع إلى أن استخدام التكنولوجيا في شركات التأمين ليس بالأمر الحديث، خاصة بالنسبة للتأمين على الحياة حتى أن العديد من الشركات في وقت مضى تدخلت في عمليات التطوير التكنولوجي وذلك نتيجة لحاجتها لتكنولوجيا لم تكن متوفرة بعد، كما أن اختراع الآلة الحاسبة وتطوير نسخ تجارية منها منح أقسام الرياضيات وإدارة المخاطر احتراماً أكبر، ولإسقاط الموضوع على التأمين فإنه على الرغم من أن أول خبير اكتواري بالمعايير الحالية كان وليام مورغان (1750-1833) إلا أن أفكاره لم تطبق بشكل عملي إلا بعد 1851 حيث تم إطلاق أول آلة حاسبة تجارية.

لذا يجب أن ننظر إلى التكنولوجيا على أنها ضرورة للبقاء والاستمرار لهذه الشركات وليست مجرد وسيلة للتقدم والتطور هذا الأمر سيغير الكثير من المفاهيم لدى القائمين على شركات التأمين.

وبالرجوع إلى التأمين التكافلي فإنه على الرغم من اختلافه مع التأمين التجاري من الجانب الشرعي من حيث عدم احتوائه على كل من الغرر والرهان والربا إلا أنه يتقاطع مع التأمين التجاري في الكثير من المبادئ والخصائص الأساسية فكل النوعين يشار إليهما بما يلي:

- توصف الهيئات التي تقوم بالعملية التأمينية بأنها هيئات ذات ثقة مالية، ويقصد بذلك أنه عندما تتعاقد هذه الهيئات على تأدية التأمينية خدمات التأمين فإن تعاقدتها هذا يجب أن يكون موثقاً بدون أن يحتاج إلى أي ضمان أو رهن بل يكفي كتابة العقد ودفع القسط، (سلامة، 1967، الصفحات 26-27).
- تتميز العملية التأمينية منذ الإعلان عن طبيعتها وتسويقها إلى أداء المطالبات باعتمادها على خبرات فنية متخصصة و متميزة عن غيرها من الخبرات الموجودة بالمشايخ الخدماتية الأخرى-ونقص هذا الخبرة الإكتوارية.(علي و منى، 1994، صفحة 12)
- إن نجاح عمل شركة التأمين مهما كان نوعها يعتمد على قانون الأعداد الكبيرة من جهة وعلى ضخامة البيانات التي تمتلكها من جهة أخرى، هذه البيانات التي تختلف من حيث درجة خصوصيتها وأهميتها لدى أصحابها، والتي تعتبر وجبة دسمة للمخترقين.

وعلى الرغم من عدم تواجد دراسات تتناول المخاطر السيبرانية في شركات التأمين التكافلي فإنه في نفس السياق لا توجد دراسات تشير إلى اختلاف المخاطر السيبرانية التي تتعرض لها شركات التأمين التكافلي عن نظيرتها التجارية، وهذا هو الطرح الذي سنعتمد عليه في محاولة الإجابة على إشكالية هذه الدراسة والمتمثل في:

"فيما تتجلى المخاطر السيبرانية في شركات التأمين التكافلي وكيف يمكن التعامل معها؟"

وللإجابة على هذه الإشكالية تم سنحاول الإحاطة بمعطيات الدراسة من خلال نقطتين أساسيتين، تتمثل الأولى في المخاطر السيبرانية وماهيتها وكيف تتجلى في شركات التأمين، أما الثانية فقد تطرقنا فيها للتعامل مع المخاطر سواء من وجهة النظر الإشرافية أو من وجهة النظر الاكتوارية.

## 1. المخاطر السيبرانية في شركات التأمين

وسنعالج الموضوع من خلال النقاط التالية:

## 1.1. أساسيات حول الموضوع

هناك بعض النقاط التي يجب أن نوضحها في البداية لتحديد مجال انتماء هذا النوع من المخاطر له أهمية قصوى ، كما أننا نشدد على درجة الخطورة البالغة للمخاطر السيبرانية على قطاع التأمين مقارنة مع بقية القطاعات .

## أولاً: إلى أين تنتمي المخاطر السيبرانية في شركات التأمين التكافلي

على الرغم من أن شركات التأمين التكافلي تتعرض لمخاطر خاصة بها تتعلق بطبيعة عملها إلا أنها تتشارك مع شركات التأمين التجاري في جملة واسعة من المخاطر، خاصة المخاطر التشغيلية والتي تعتبر مخاطر الخسارة المترتبة عن المشاكل الناتجة عن التعاملات مع الأطراف الأخرى، أو عدم كفاءة العمليات الداخلية أو فشلها والتي تشمل: (Birla، 2008، صفحة 5). الأخطاء التي يرتكبها الموظفون، فشل الأنظمة، الحرائق والفيضانات أو غيرها من الخسائر على الأصول المادية، احتيال أو نشاط إجرامي آخر.

كما تعرف المخاطر التشغيلية حسب لجنة بازل بأنها مخاطر حدوث خسائر نتيجة فشل أو عدم ملائمة أنظمة الضبط والرقابة الداخلية الموظفين أنظمة المعلومات أو الأحداث الخارجية وتتضمن المخاطر القانونية ولا تتضمن المخاطر الإستراتيجية أو مخاطر السمعة. (الأطر الخاصة بالمخاطر التشغيلية، 2019، صفحة 5)، ومن خلال التمعن في تعريف المخاطر التشغيلية نجد بأن المخاطر السيبرانية تندرج تحت هذا النوع من المخاطر، ليس هذا فحسب بل إنها تعد أكثر أنواعها تهديداً.

أما بالنسبة لتوزيع المخاطر فقد أوضحت السلطات الإشرافية الأوروبية في تقريرها أن العنصر الأكثر خطورة في المخاطر التشغيلية للمؤسسات المالية يتعلق بالمخاطر الإلكترونية، وفيما يخص قطاع التأمين فإنها تتوزع كالتالي:

(JOINT COMMITTEE REPORT ON RISKS AND VULNERABILITIES IN THE EU FINANCIAL SYSTEM, 2021, p.

:12)

• مخاطر الرقمنة 73٪

• مخاطر الاكتتاب السيبراني 19٪

• منافسة 8٪

## ثانياً: لماذا شركات التأمين تعتبر الأعلى عرضة للهجمات الإلكترونية؟

تعتبر مجموعات التأمين هدفاً طبيعياً للهجمات الإلكترونية لأنها تمتلك كميات كبيرة من بيانات حامل وثيقة التأمين السرية لأن المنتجات والسياسات والأسعار كلها مدعومة بالبيانات. وهذا ما يجعلها ذات قيمة كبيرة، كما أنه من خلال البيانات تستطيع شركة التأمين أن تقدم للمستهلك ما يحتاجه فقط، مع أمل أن يكون ذلك بالسعر المناسب، والسبب وراء كون المستهلكين على استعداد لمشاركة بياناتهم هو المزيد من الخيارات وتكاليف أقل ، كما أنه وعلى عكس القطاعات

الأخرى التي تحتوي بشكل أساسي على بيانات مالية حساسة فقط، فإن شركات التأمين تجمع نوعين من المعلومات الحساسة لعملائها منه ما هو مالي ومنه هو شخصي. (Cyber risks: what is the impact on the insurance industry, 2021)

كما أن وباء كورونا أدى إلى تسريع التحول الرقمي. حيث زادت المؤسسات المالية من استخداماتها لتكنولوجيا المعلومات. حيث أنهم تعتمد حالياً بشكل أكبر على الحلول الرقمية لأداء عملياتها اليومية وتقديم خدماتها للعملاء. وفي حين أن هذا قد يجلب الفوائد أكبر، إلا أن الاعتماد المتزايد على الحلول الرقمية زاد أيضاً من مخاطر الهجمات الإلكترونية، حيث تعتبر المخاطر السيبرانية من أهم المخاطر العالمية على القطاع المالي والاقتصاد ككل. وعلى الرغم من أنه لم يتغير نوع مخاطر تكنولوجيا المعلومات والاتصالات التي تتعرض لها المؤسسات في السنوات الماضية، إلا أنه قد زاد تواتر الحوادث وحجم تأثيرها على الكيانات المالية، وقد كشفت دراسة حديثة بعنوان Covid-19 والمخاطر الإلكترونية في القطاع المالي - أن القطاع المالي قد شهد أكبر عدد من الأحداث الإلكترونية في فترة Covid-19 بعد القطاع الصحي، ومؤسسات الدفع وشركات التأمين والاتحادات الائتمانية هي الأكثر تضرراً في هذا القطاع (Jon & Leonardo , 2021, p. 6) :

## 2.1. أنماط التهديدات السيبرانية ونتائجها المحتملة

إن المقام في الحقيقة لن يتسع لتناول كل المخاطر السيبرانية كما أن التركيز على نوع دون الآخر لن يخدم البحث، لذا ارتأينا أن نتناولها في أغلها بشكل مختصر، مع محاولة توضيح نتائجها المحتملة على شركات التأمين، إلا أنه لابد أن نقوم في البداية توضيح ماهية التهديدات السيبرانية، إلى جانب توضيح المفاهيم ذات الصلة.

### أولاً: مفاهيم سيبرانية

وستتناول فيما كل من: مفهوم الفضاء السيبراني، الخطر أو التهديد السيبراني، الأمن السيبراني

#### • مفهوم الفضاء السيبراني

يعرف على أنه المجال المادي وغير المادي الذي يتكون من عناصر تتمثل في أجهزة الكمبيوتر والشبكات والبرمجيات وحوسبة المعلومات والمحتوى ومعطيات النقل والتحكم ومستخدمو كل هذه العناصر، حيث تعد هذه العناصر العامل المشترك في جميع محاور استخدام الفضاء السيبراني، سواء أكانت الجهات المستخدمة قادرة على تعظيم قيمها وقدراتها بما في ذلك رفع كفاءة العنصر البشري أم كانت في مرحلة متأخرة. (نورة ، 2018 ، صفحة 190).

#### • مفهوم الخطر السيبراني

خطر الأمن السيبراني هو الضرر المحتمل أو تدمير أصول الأعمال والإيرادات والسمعة. يحدث هذا الضرر من قبل المهاجمين البشريين الذين يحاولون سرقة المال أو المعلومات أو التكنولوجيا.

وفي حين أن هذه الهجمات تحدث في البيئة التقنية، فإنها غالباً ما تمثل خطراً على الجهة المصابة بأكملها. لذا يجب مواءمة المخاطر مع إطار عمل قياس المخاطر وتتبعها والتخفيف منها. ولا تزال العديد من المؤسسات تتعامل مع مخاطر الأمان عبر الإنترنت على أنها مشكلة تقنية يجب حلها ويؤدي هذا التصور إلى استنتاجات خاطئة لا تخفف من تأثير الأعمال الاستراتيجية للتعامل مع المخاطر (رؤى إدارة المخاطر، 2022)

### • مفهوم الأمن السيبراني

أما الأمن السيبراني فيعرف على أنه مجموعة التقنيات والممارسات والعمليات المصممة للحفاظ على الشبكات، البرامج والأجهزة والبيانات من التلف أو الهجوم أو الوصول غير الرسمي (Reetu , 2021, p. 1)

كما عرفه إدواردو أمورسو بأنه: وسائل من شأنها الحد من خطر الهجوم على البرمجيات وأجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل والأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها وتوفير الاتصالات المشفرة (الأمن السيبراني، 2021، صفحة 1).

وقدمت وزارة الدفاع الأمريكي البنتاغون تعريفا دقيقا لمصطلح الأمن السيبراني فاعتبرته جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية من مختلف الجرائم: الهجمات، التخريب التجسس والحوادث. (فارس و ابراهيم ، 2022 ، صفحة 16)

### ثانيا: أنماط الهجمات السيبرانية

قد يطول الشرح بخصوص المخاطر السيبرانية، لذا ارتأينا أن نعتمد الجدول التالي والذي يوضح أنواع التهديدات والنتائج المترتبة عنها

الجدول رقم (1): أنماط التهديدات السيبرانية

| التهديدات                               | الوسائل                                                      | النتيجة                                                                                                                                                                                                                                                             |
|-----------------------------------------|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| التخريب                                 | ✓ البرمجيات الخبيثة<br>✓ الاختراق<br>✓ اغراق الخادم بالطلبات | ✓ تعطل الخدمات<br>✓ تخريب الأجهزة<br>✓ تدمير البنية التحتية                                                                                                                                                                                                         |
| سرقة البيانات واستغلال الحسابات الشخصية | ✓ الاختراق<br>✓ الهندسة الاجتماعية<br>✓ التصيد الإلكتروني    | ✓ الحصول على، مستندات صور أو ملفات هامة<br>✓ سرقة الأموال والحسابات<br>✓ سرقة الهوية بهدف الحصول على قروض بنكية أو إتمام معاملات مالية باسم الضحية<br>✓ سرقة عناوين، أرقام تليفون وعناوين البريد الإلكتروني الخاصة بالأصدقاء والمعارف بهدف استهدافهم بحملات إعلانية |
| التجسس                                  | ✓ البرمجيات الخبيثة<br>✓ الاختراق                            | ✓ السيطرة الكاملة على الأجهزة، حتى إنها تسمح للمخترقين بالاطلاع على كافة محتويات الهاتف والتجسس على المستخدمين دون علمهم                                                                                                                                            |

المصدر: (أيمن ، صفحة 8)

### 3.1. نتائج تحقق الهجمات السيبرانية

يمكن أن نصنف الأضرار الناتجة عن تحقق الهجمات السيبرانية إلى ثلاثة مجالات:

#### أولاً: فقدان البيانات السرية

قد تتضمن معلومات التعريف الشخصية التي تجمعها وتخزنها شركات التأمين، بما في ذلك المعلومات الصحية الشخصية لحاملي وثائق التأمين، وفي بعض الحالات، لأطراف ثالثة، الأسماء وتواريخ الميلاد وأرقام الضمان الاجتماعي وعناوين الشوارع والبريد الإلكتروني وأرقام التعريف الطبية وبيانات التوظيف مثل كدخل. قد تكون السجلات الصحية الخاصة ذات قيمة خاصة في الأسواق السوداء كأدوات للاحتياز والاحتيال وسرقة الهوية مما يجعل شركات التأمين التي تجمع هذه المعلومات أهدافاً ذات قيمة عالية للمجرمين

بالنسبة لحاملي وثائق التأمين التجارية، قد تقوم شركات التأمين بجمع معلومات تجارية حساسة قد تكون ذات قيمة بالنسبة للشركات والجواسيس الأجانب. في حالة منتجات التأمين على الإنترنت، على سبيل المثال قد تمتلك شركات التأمين معلومات حول ضوابط أمان الشبكة لحامل بوليصة التأمين وغيرها من معلومات المرونة الإلكترونية التي يمكن أن تكون ذات قيمة للقراصنة وغيرهم من مجرمي الإنترنت.

علاوة على ذلك، قد يؤدي فقدان المعلومات السرية إلى الإضرار بحقوق الملكية الفكرية القيمة لحامل الوثيقة.

#### ثانياً: تعطيل الأعمال

لا تنطوي جميع حوادث الأمن السيبراني على انتهاكات للبيانات؛ يمكن أن تؤدي بعض الهجمات الإلكترونية إلى تعطيل العمليات التجارية العادية. وكمثال على ذلك فقد تم الإبلاغ عن حادثة هجوم السيبراني على شركة Sony Pictures دمرت شبكة الشركة بالكامل، بما في ذلك رسائل البريد الإلكتروني وأدلة الهاتف ورسائل البريد الصوتي وسجلات الأعمال مثل قوائم العقود، وكانت تكاليف الاسترداد الكبيرة.

#### ثالثاً: الإضرار بالسمعة

أساس عمل التأمين هو ثقة حامل الوثيقة- ثقب بأن المعلومات التي تجمعها شركات التأمين ستتم حمايتها، وثق في أن المطالبات سيتم سدادها في الوقت المناسب عندما يكون ذلك مناسباً - فإذا كانت شركة التأمين تعاني من خرق للبيانات، قد يؤدي إلى كشف معلومات صاحب الترخيص السرية، فقد تتزعزع تلك الثقة. وبالمثل، إذا تعرضت شركة التأمين لحادث أمن إلكتروني جعلها غير قادرة على سداد مدفوعات المطالبات في الوقت المناسب أو أوقفتها بطريقة أخرى قد تتزعزع هذه الثقة أيضاً. ويمكن أن تمتد مخاطر السمعة إلى قطاع التأمين ككل وتؤثر سلباً على ثقة المستهلكين وحملة وثائق التأمين والمستثمرين ووكالات التصنيف والشركاء التجاريين.

## 2. طرق التعامل مع المخاطر السيبرانية في قطاع التأمين

إن الإجراءات المتبعة في هذا السياق يمكن أن تأخذ ثلاثة مناحي مختلفة، المنحى الأول يتعلق بطريقة التعامل مع هذه المخاطر، أما المنحى الثاني فيتعلق بما أقرته الجهات الإشرافية والرقابية الدولية، فلا ننسى أن قطاع التأمين من القطاعات شديدة الحساسية والتي تخضع لرقابة شديدة، أما المنحى الثالث فيتعلق بالطريقة المتبعة من قبل الخبراء الإكتواريين لمواجهة هذا النوع من المخاطر

### 1.2. كيفية التعامل مع المخاطر السيبرانية

سننتقل إلى هذه النقطة من خلال

- كيف نتعامل مع طبيعة الخطر
- كيف نتعامل مع مصدر الخطر

#### أولاً: كيفية التعامل مع طبيعة الخطر

إن سؤال أي متخصص في مجال الأمن عن خيارات إدارة المخاطر، فإن من المرجح أن تكون الإجابات متشابهة. حيث يتفق المتخصصون الأمنيين ومديرو المخاطر في جميع التخصصات بشكل عام على وجود أربعة خيارات للتعامل مع المخاطر. في حين أن الأسماء والأوصاف قد تختلف من صناعة إلى أخرى، فإن الطرق الأربعة المقبولة عالمياً للتعامل مع المخاطر هي:

- التجنب (الابتعاد عن المساعي المحفوفة بالمخاطر)
- التخفيف (تأسيس العمليات والإجراءات والأنظمة لتقليل المخاطر)
- التحويل (الاستعانة بمصادر خارجية، عادة عن طريق التأمين، المخاطر إلى كيان آخر)
- القبول (اغتنم الفرص المرتبطة باحتمالية وقوع الحدث)

#### ثانياً: كيفية التعامل مع مصدر الخطر

حتى يتحقق الهدف من الأمن السيبراني، لا بد من توفر مجموعة من العناصر مع بعضها البعض لتكتمل الدور في ذلك، ومن أهم أبعاد وعناصر الأمن السيبراني: (إيمان، 2022)

- التقنية: (technology) تشكل التكنولوجيا والتقنية دوراً في غاية الأهمية في حياة الأفراد والمنظمات، حيث توفر الحماية الفائقة لهم أمام الهجمات السيبرانية، وتشتمل حماية الأجهزة بمختلف أشكالها الذكية والحاسوبية والشبكات بالاعتماد على جدران الحماية واستخدام البرامج الضارة ومكافحة الفيروسات وغيرها.
- الأشخاص: (People) يستوجب الأمر لزوماً على الأشخاص من مستخدمي البيانات والأنظمة في منشأة ما استخدام مبادئ حماية البيانات الرئيسية كتحديد كلمة مرور قوية، وتفادي فتح الروابط الخارجية والمرفقات عبر البريد الإلكتروني، إلى جانب القيام بعمل نسخ احتياطية للبيانات.

- الأنشطة والعمليات (Process): يتم توظيف الأشخاص والتقنيات للقيام بالعديد من العمليات والأنشطة وتسييرها بما يتماشى مع تطبيق أسس الأمن السيبراني والتصدي لهجماته بكل كفاءة.

كما نضيف لما سبق عنصر أساسي وهو السياسات والقائمين على هذا المجال يفهمون أن التكنولوجيا الجيدة لا تفيد كثيرًا بدون سياسة مقابلة وفعالة بنفس القدر. حيث لن توفر التكنولوجيا وحدها الحماية الكافية ضد معظم أنواع الهجمات. هناك العديد من الحالات التي يمكن أن تؤثر بها السياسة قيمة التكنولوجيا. فترك قاعدة البيانات مكشوفة في السحابة بسبب سياسة غير واضحة سيقوض أي تحكم متطور في الوصول أو سيلغي فاعلية تقنية حماية المحيط.

وهناك نقطة أخرى وتعلق بالجانب البشري، باعتباره عنصر أساسي في سلسلة الأمن السيبراني، إلا أن هذا العنصر يعتبر الحلقة الأضعف في هذه السلسلة لذلك لا بد من التركيز في التعامل معه. وتؤكد إحدى الدراسات أن معظم الهجمات تعتمد على شكل من أشكال الهندسة الاجتماعية (Steven, 2022) وأن نجاح أي هجوم من نمط الهندسة الاجتماعية، يكون دائمًا نتيجة لتدريب المستخدم غير الكافي. يعتمد مجرمو الإنترنت على قدرتهم على خداع المستخدمين لتقديم المعلومات.

## 2.2. الرقابة والإشراف على المخاطر السيبرانية

يعتمد هذا القسم على ورقة تطبيق IAIS حول الإشراف على الأمن السيبراني لشركة التأمين عدد من المنظمات الدولية والوطنية والصناعية في القطاعين العام والخاص وضع القطاع أطراً وإرشادات للأمن السيبراني ذات صلة بالتأمين. أما بالنسبة للمصادر الرئيسية التي يمكن لمشرفي التأمين الرجوع إليها في عملية الإشراف على الجانب السيبراني فنجد الموارد التالية:

- العناصر الأساسية لمجموعة السبع للأمن السيبراني للقطاع المالي (G7FE)

(G7 FUNDAMENTAL ELEMENTS OF CYBERSECURITY, 2016)

- العناصر الأساسية لمجموعة السبع ذات الصلة للتقييم الفعال للأمن السيبراني للقطاع المالي

(G7FEA

(G-7 FUNDAMENTAL ELEMENTS FOR EFFECTIVE ASSESSMENT, 2017)

- إرشادات حول المرونة السيبرانية للبنى التحتية للأسواق المالية دليل (CPMI-IOSCO) والمقصود المرونة "هو القدرة على توقع هجوم إلكتروني ومقاومته واحتوائه والتعافي منه بسرعة.

(CPMI-IOSCO, Guidance on Cyber Resilience for Financial Market Infrastructures, 2016)

ويمكن اعتبار ما جاء في الموارد السابقة مجموعة موجزة لمبادئ الأمن السيبراني غير الملزمة للكيانات العامة والخاصة في القطاع المالي. والهدف منها هو إفادة كل من الشركات والمشرفين. وقد تم تحديد العناصر الأساسية الثمانية من قبل G7 وتمثل المبادئ في العناصر التالية: 1. إستراتيجية وإطار الأمن السيبراني 2. الحوكمة 3. تقييم المخاطر والرقابة، 4. المراقبة، 5. الاستجابة، 6. الانتعاش، 7. تبادل المعلومات، 8. التعلم المستمر.

### 3.2. العلوم الاكتوارية والأمن السيبراني

قد يغيب عن البعض أن أحد أهم وظائف الخبراء الاكتواريين وأكثرها تخصصا هو إدارة المخاطر في المؤسسات وباعتبار أن الخبير الاكتواري يعتبر مدير المخاطر في أعرق شركات التأمين فإن الطريقة التي يتعامل بها هذا النوع من الخبراء مع الخطر عموما والخطر السيبراني خصوصا يجب أن تدرس وأن يتم الاستفادة منها حتى بالنسبة للشركات التي لا يمكنها توظيف هذا النوع من المتخصصين.

#### أولا: مفهوم الخبير الاكتواري

حسب الجمعية الدولية للإكتواريين "الإكتواري هو مفكر متعدد المواصفات الإستراتيجية، متمرس في النظريات والتطبيقات في علوم الرياضيات والإحصاءات والاقتصاد وحساب الاحتمالات والعلوم المالية. لُقّب الإكتواري بالمهندس المالي ومهندس الرياضيات الاجتماعية، لأن تركيبته الفريدة التي يتحلّى بها من تحليل وصفات عمل تسمح له بمواجهة التحديات المالية والاجتماعية في العالم كله. (راشد، 2005، صفحة 2)

ويمكن أن نعرف الإكتواري على أنه "كل شخص يقوم بدراسات اقتصادية ومالية وإحصائية بهدف إعداد أو تغيير عقود التأمين، ويقوم بتقييم أضرار وتكاليف المؤمن والمؤمن له، ويحدد أسعار الاشتراك بالسهر على مردودية الشركة ويتابع نتائج الاستغلال ويراقب الاحتياطات المالية للشركة". (الأمر 07/95 المؤرخ في 25 جانفي 1995، المتعلق بالتأمينات، 1995، صفحة 35)

ويمكن أن نعرفه على أنه "شخص متخصص ذو مهارة عالية، وهو على دراية بكل جوانب عمل شركات التأمين والتي تشمل التخطيط والتسعير والبحوث". (ريجدا، 2006، صفحة 805)

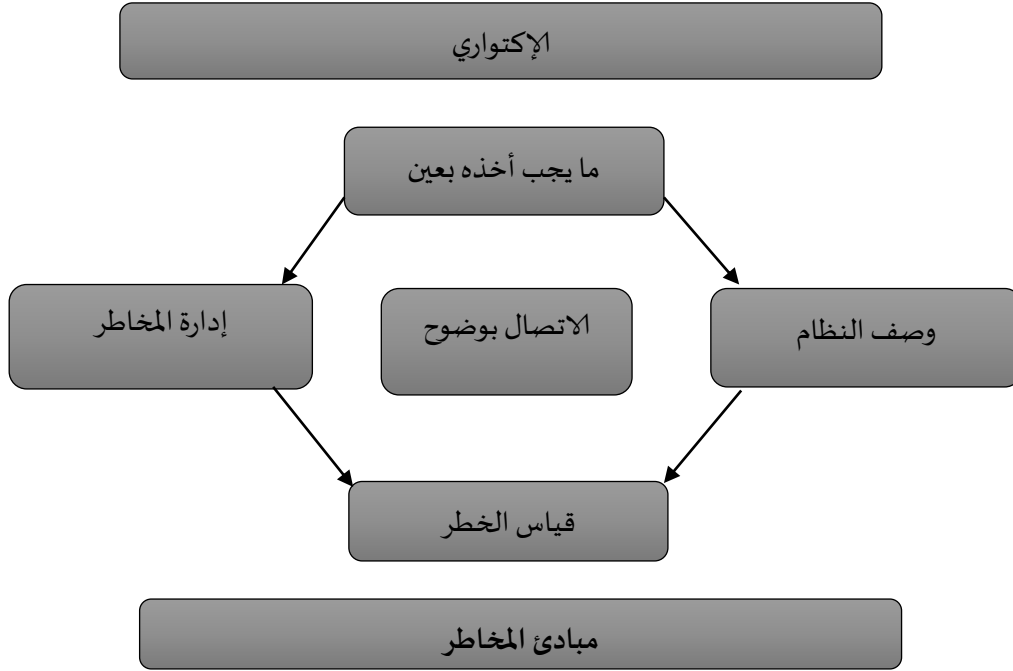
#### ثانيا: توظيف الخبرة الاكتوارية في مجال الأمن السيبراني

- يحاول الخبراء الاكتواريون تحديد المخاطر باستخدام تحليل الاحتمالات لتحديد تأثيرها الاقتصادي.
- العديد من الشركات في صناعة التأمين توظف خبراء اكتواريين -مختبرين يقومون بتقييم وإدارة مخاطر الاستثمارات المالية، وغيرها من المشاريع التي يحتمل أن تكون محفوفة بالمخاطر.
- يطبق هؤلاء الخبراء الاكتواريون تقنيات العلوم الاكتوارية لفهم المسؤوليات المرتبطة بوثائق التأمين على الأمن السيبراني وكذلك الهجمات الإلكترونية نفسها.

وعلى الرغم من أنه لم تثبت صناعة التأمين أنها تتمتع بميزة عندما يتعلق الأمر بالحماية من الهجمات الإلكترونية-مع ذلك-فإن الفهم العميق للمخاطر داخل هذا القطاع يسمح للعديد من شركات التأمين باتخاذ قرارات مستنيرة حول مقدار المخاطر الإلكترونية التي يجب تجنبها أو تخفيفها أو نقلها إلى شركة تأمين أخرى أو التي يمكن قبولها. (Steven, 2022)

والشكل الموالي يوضح طريقة تعامل الخبراء الاكتواريين مع المخاطر بصفة عامة

الشكل رقم (1): إدارة المخاطر من وجهة نظر إكتوارية



المصدر: (Risk management– an actuarial approach, 2017, p. 3)

أما بالنسبة لإسقاطها على قطاع التأمين فإنه يتم كالتالي: (Risk management– an actuarial approach, 2017, p. 6)

#### • ماذا يجب أن نأخذ بعين الاعتبار

ترتبط مخاطر الإنترنت بمجموعة واسعة جداً من المنظمات والأفراد، وفي العادة فإنه عندما يقدم الخبراء الاكتواريون المشورة بشأن المخاطر، فمن المرجح أن يكون صاحب المصلحة الرئيسي - شركة تأمين أو صندوق تقاعد-، لكن الخبراء الاكتواريين حالياً يؤدون أعمالهم بشكل متزايد في "مجالات أوسع"، ويقدمون المشورة للشركات المالية الأخرى وكذلك الشركات غير المالية.

وبغض النظر عن قد يكون صاحب المصلحة الرئيسي فمن المهم توضيح درجة قلقه المحتملة بشأن المخاطر الإلكترونية (والتي قد تكون مرتبطة أيضاً بوعي أصحاب المصلحة بالتعرض المحتمل للمخاطر الإلكترونية). فإذا كان واثقاً جداً من قدرته على تجنب هذه المخاطر، فإنه غير المرجح أن يستثمر كثيراً في السيطرة عليها - والعكس صحيح.

من المهم أيضاً النظر في كيفية ظهور المخاطر، فعلى سبيل المثال، عندما تتحقق إحدى المخاطر السيبرانية لمنظمة ما يمكن أن يواجه:

➤ التكاليف المباشرة: مثل الاستعانة بالاستشاريين أو الدفع الغرامات.

- التكاليف غير المباشرة : مثل التحقيقات الداخلية ، أو التباطؤ في معدل اكتساب عملاء جدد.
- تكاليف الفرصة ، مثل انخفاض ثقة العملاء والإضرار بالسمعة

وهنا يحتاج مديرو المخاطر – عادة ما يكونون إكتواريين - إلى فهم أعمال أصحاب المصلحة وأي من هذه التكاليف سيكون مصدر قلق أكبر بالنسبة لهم المصدر.

#### • وصف النظام

بعد رسم صورة لأصحاب المصلحة ومواقفهم من المخاطر ، يمكن لمدير المخاطر البدء في تمهيد الطريق لتحليل وقياس المخاطر السيبرانية.و تتمثل المرحلة الأولى في التحدث إلى الخبراء في المنظمة لبناء صورة دقيقة لمدى احتمالية تعرضها للمخاطر الإلكترونية، وهؤلاء الخبراء يجب أن يمثلوا مجالات مختلفة ، مثل الحوكمة وتكنولوجيا المعلومات والمبيعات إلى جانب الاستعانة بمصادر خارجية .

ومن ثم لا بد من التركيز على المخاطر السيبرانية التي يمكن أن تنشأ من مجموعة متنوعة من المصادر الداخلية والخارجية على حد سواء، ويتيح جمع المعلومات التفصيلية لمدير المخاطر تحديد المخاطر ذات الأولوية والتي يجب تحليلها .قد يكون لبعض المخاطر السيبرانية تأثير أكبر مجتمعة من تأثيرها بمفردها ومن المهم فهم هذه الروابط .لأن معرفة المخاطر الإلكترونية الرئيسية وكيفية تفاعلها سيساعد في المخاطرة المدراء لبناء نموذج أولي للمخاطر.

#### • قياس المخاطر

لا ينبغي أن يبرز نموذج المخاطر الإلكترونية الفعال فقط النتائج الأكثر احتمالية ولكن أيضًا النتائج الأكثر تطرفًا والتي يمكن أن تمثل مع ذلك خسائر كبيرة للغاية .عندما تحدث المخاطر السيبرانية، يمكن أن يحدث التأثير في مراحل مختلفة على سبيل المثال، فإنه مباشرة بعد الهجوم الإلكتروني، الشركة المتضررة ستغلق التطبيق المخترق وتعيين المزيد من الموظفين للتعامل مع الاستفسارات، في وقت لاحق، التركيز يمكن أن يكون على إدارة التأثير عن طريق تعديل الأقساط وتحسين الأمن السيبراني؛ في وقت آخر قد تحتاج الشركة إلى تغيير القرارات الإستراتيجية، على سبيل المثال التراجع عن انتهاج سياسة استحواذية لأن الحدث الإلكتروني أدى إلى انخفاض التصنيف الائتماني، لذلك من المهم توضيح الأفق الزمني الذي يعتبر مهم لأصحاب المصلحة من أجل التقييم الكامل للإمكانات والآثار المترتبة على حدوث خطر.

#### • إدارة المخاطر

إن عملية الوصف ثم القياس والنمذجة يجب أن تعطي للمؤسسة صورة واقعية عن تعرضها للمخاطر السيبرانية، جنبًا إلى جنب مع السيناريوهات المتوقعة وتأثيراتها. ليتم تحويل هذه المعلومات إلى خطة عمل لإدارة المخاطر السيبرانية، كما يجب على الشركة الآن تفسير ذلك دليل في سياق قدرتها على تحمل المخاطر.

غالبًا ما يكون للمنظمة مجال لتحسين العمليات الداخلية من أجل التخفيف جوانب المخاطر السيبرانية. تشمل الأمثلة توضيح مدى خطورة المخاطر الإلكترونية على مستوى مجلس الإدارة، تنفيذ تكنولوجيا المعلومات ضوابط؛ ترتيب البيانات الداخلية حسب مستوى الضرر المحتمل إذا تم اختراقها؛ أو الحد من العلاقات مع الموارد التي ينظر إليها على أنها مخاطرة عالية .

## خلاصة

بعد الطرح الذي قدمناه والذي تناولنا من خلاله موضوع المخاطر السيبرانية في شركات التأمين بصفة عامة وفي شركات التأمين التكافلي بصفة خاصة توصلنا إلى جملة من النتائج يتلخص أهمها في:

- حداثه شركات التأمين التكافلي مقارنة بنظيرتها التقليدية يجعلها أقل خبرة في مجال التكنولوجيا والتعامل مع مخاطرها، لذا سيكون من المناسب محاولة عدم الإفراط في الاستفادة من التكنولوجيا والتدرج في ذلك.
- في الحقيقة فإن المخاطر السيبرانية ليست تهديدا حقيقيا بسبب وجودها فحسب بل إن تفاقمها و زيادة أعداد الهجمات الإلكترونية ساهم في زيادة خطورتها و شدة نتائجها.
- إن الهندسة الاجتماعية تعد السبب الرئيسي للمخاطر السيبرانية ذلك راجع إلى أنه من السهل التلاعب والتحكم بالعنصر البشري كما أن الإهمال عامل وارد جدا لذلك هناك ضرورة ملحة للتركيز على تدريب الموظفين، و تحذيرهم من الهندسة الاجتماعية وطرق مواجهتها.
- لا ننسى أن التأمين الإلكتروني يعتبر إحدى الامتيازات والفرص الناشئة عن التحول الرقمي، إلا أن هذا التحول يحمل تحديات أساسية لشركات التأمين: التحدي الأول حول طبيعة نظام التأمين الإلكتروني وصعوبة تسعيره، أما التحدي الثاني فيتجسد في صعوبة توفير متخصصين متأهلين في وسعهم تقديم المشورة والتوجيهات للمؤسسات المؤمنة بخصوص هذا النوع من التأمين.

## Bibliography

1. Steven, B. (2022, 11 10). Cybersecurity in the insurance industry. Retrieved from <https://cybersecurityguide.org/industries/insurance/>
2. Birla, N. (2008). risks faced by general insurers. 10 th global conference of actuaries.
3. (2016). CPMI-IOSCO, Guidance on Cyber Resilience for Financial Market Infrastructures. Basel: Bank for International Settlements.
4. Cyber risks: what is the impact on the insurance industry. (2021, 10 15). Retrieved from [www.eiopa.europa.eu: https://www.eiopa.europa.eu/media/feature-article/cyber-risks-what-impact-insurance-industry\\_en](https://www.eiopa.europa.eu/media/feature-article/cyber-risks-what-impact-insurance-industry_en)
5. G-7 FUNDAMENTAL ELEMENTS FOR EFFECTIVE ASSESSMENT. (2017, 10 26). Retrieved from <https://www.bundesbank.de: https://www.bundesbank.de/resource/blob/665510/3a6628d69698bf3bb04bf94629f0ac84/mL/2017-10-26-g7-fe-for-effective-assessment-data.pdf>
6. G7 FUNDAMENTAL ELEMENTS OF CYBERSECURITY. (2016, 10). Retrieved from [https://www.ecb.europa.eu: https://www.ecb.europa.eu/paym/pol/shared/pdf/G7\\_Fundamental\\_Elements\\_Oct\\_2016.pdf?69e99441d6f2f131719a9cada3ca56a5](https://www.ecb.europa.eu: https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf?69e99441d6f2f131719a9cada3ca56a5)
7. (2021). JOINT COMMITTEE REPORT ON RISKS AND VULNERABILITIES IN THE EU FINANCIAL SYSTEM. uropean Securities and Markets Authority.
8. Jon, F., & Leonardo , G. (2021). Covid-19 and cyber risk in the financial. Basel: Bank for International Settlements.
9. Reetu , S. (2021). A REVIEW ON CYBER SECURITY. International Journal of Advance and Innovative Research, 8(2).
10. (2017). Risk management– an actuarial approach. Institute and Faculty of Actuaries (IFoA).

11. Tom, J. (2021, 1 11). Cybersecurity Insurance Has a Big Problem. Retrieved from <https://hbr.org/https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem>
12. أحمد شاكر علي، و محمد عمار منى. (1994). إدارة ومحاسبة منشآت التأمين. القاهرة: جامعة القاهرة مركز التعليم الفتوح.
13. (2019). الأطر الخاصة بالمخاطر التشغيلية. أبو ضبي: صندوق النقد العربي.
14. الأمر 07/95 المؤرخ في 25 جانفي 1995، المتعلق بالتأمينات. (1995). الجريدة الرسمية الجزائرية (13)، 2-36.
15. (2021). الأمن السيبراني. الأردن: هيئة الإعلام قسم الدراسات والاتصال والعلاقات العامة.
16. العمارات فارس ، و محمد الحمامصة ابراهيم . (2022). الامن السيبراني (المفهوم وتحديات العصر. عمان: دار الخليج للنشر والتوزيع.
17. جورج ريجدا. (2006). إدارة الخطر والتأمين. (توفيق البلقيني محمد، و محمد مهدي ابراهيم، المترجمون) الرياض: دار المريخ.
18. رؤى إدارة المخاطر. (2022, 09 22). تم الاسترداد من <https://learn.microsoft.com:https://learn.microsoft.com/ar-sa/azure/cloud-adoption-framework/secure/risk-insights>
19. سليم راشد راشد. (2005). القواعد والمعايير الدولية الراجعة لدور الإكتواري. مؤتمر آفاق التأمين. دمشق.
20. شلوش نورة . (2018). القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول. مجلة مركز بابل للدراسات الإنسانية، 2(8).
21. عبد الله سلامة. (1967). إدارة وتنظيم منتجات التأمين (الإصدار 3). القاهرة: دار النهضة العربية.