Trabajo Fin de Máster

¿Es posible construir un modelo homogenizado para evaluar primas de seguros cibernéticas en Europa para instituciones financieras?

Autor Lucas Engl

Máster Universitario en Banca y Finanzas UPF Barcelona School of Management

Curso 2019 – 2020

Mentor Miquel Planiol Ribera

BARCELONA SCHOOL OF MANAGEMENT

¿Es posible construir un modelo homogenizado para evaluar primas de seguros cibernéticas en Europa para instituciones financieras?

Proyecto desarrollado en el marco del programa **Máster Universitario en Banca y Finanzas Nombre del programa** impartido por la Barcelona School of Management centro adscrito a la Universidad Pompeu Fabra

ÍNDICE

RECONOCIMIENTOS

Esta investigación no hubiera sido posible sin la gran ayuda y el apoyo de algunas personas, lo que realmente aprecio.

En primer lugar, me gustaría agradecer a mi familia, especialmente a mi madre y a mi padre, por todo su apoyo emocional y financiero durante los últimos años, para poder cumplir mis sueños y ambiciones. También quiero agradecerle a mi mujer, Helena, por su apoyo incondicional todos los días, tanto buenos como malos. Te amo.

Además, quería agradecer a mis compañeros de trabajo, por toda su información y sugerencias sobre cómo puedo presentar los temas de la mejor manera posible.

Un agradecimiento especial a mi manager, Michael Wyss, por darme la oportunidad de trabajar en un trabajo donde amo lo que hago todos los días.

Por último, pero no menos importante, quería agradecer a la UPF y la BSM por brindarme una excelente educación en este último año, a pesar de las circunstancias, dado el COVID19.

ABSTRACTO

La Primera Revolución Industrial utilizó energía de agua y vapor para mecanizar la producción. La Segunda usó energía eléctrica para crear producción en masa. La Tercera utilizó electrónica y tecnología de la información para automatizar la producción. Ahora, una cuarta revolución industrial se basa en la Tercera. Se caracteriza por una fusión de tecnologías que difumina las líneas entre las esferas física, digital y biológica.

La velocidad de los avances actuales no tiene precedentes históricos. En comparación con las revoluciones industriales anteriores, la Cuarta está evolucionando a un ritmo exponencial en lugar de lineal. Además, está afectando a casi todas las industrias en todos los países. La amplitud y profundidad de estos cambios anuncian la transformación de sistemas completos de producción, gestión y gobierno.

En este trabajo, traté de abordar un tema muy novedoso, no solo para el sector financiero, sino también para toda la economía mundial. La digitalización y el internet de las cosas son los frutos de la cuarta revolución, y traen muchas experiencias nuevas. Obviamente, amenazas se juntan con oportunidades, y a veces es difícil mantener una visión general de los desarrollos actuales. Cyber sería uno de esos temas, que tiene el potencial de cambiar el mundo. Con el seguro cibernético, el sector financiero creó un nuevo producto, muy ajeno a finanzas, para resolver un problema que aún no ha evolucionado por completo.
De todos modos, debido a sus características particulares y su corto tiempo de vida, todavía hay muchos problemas con los procesos, la evaluación, la competencia y las expectativas relacionadas con las pólizas cibernéticas.

Con el fin de contribuir a una posible solución a este problema más amplio, tenía la intención de crear una herramienta, que mejoraría ligeramente los procesos y potencialmente homogeneizaría este mercado joven de cierta manera, con el resultado final de educar a las partes involucradas y conocer el producto de una manera más tangible.
Por lo tanto, en base a diferentes puntos de vista, limitaciones específicas y factores predeterminados, decidí crear una herramienta de calificación para las primas de pólizas cibernéticas de las instituciones financieras en Europa, preguntando la cuestión si es posible conseguir un modelo que nos dé resultados confiables.

TABLAS Y FIGURAS

Terminología	Definición
Cyber	El riesgo puede definirse como cualquier tipo de riesgo derivado del uso de datos electrónicos y su transmisión, incluidas las herramientas tecnológicas como Internet y las redes de telecomunicaciones.
Data Breach	Filtración de datos: la divulgación intencional o no intencional de información segura o privada / confidencial a un entorno no confiable.
Underwriter	Algunas instituciones financieras grandes, como bancos, compañías de seguros y casas de inversión, prestan servicios de suscripción, por lo que garantizan el pago en caso de daños o pérdidas financieras y aceptan el riesgo financiero de responsabilidad derivada de dicha garantía. Underwriter = suscritor
IoT	El internet de las cosas es un concepto que se refiere a una conexión digital de objetos cotidianos con internet
TI	Tecnología informática
Hacker	Un hacker es alguien que descubre las vulnerabilidades de una computadora o un sistema de comunicación e información

INTRODUCCIÓN

Desde ya un año estoy trabajando en el sector financiero, mas preciso, en el sector de seguros especiales corporativos. Justo después de empezar a trabajar en mi nueva posición de underwriter en Tokio Marine, una de las 20 aseguradoras mas grandes del mundo con sede en Japón y los EE.UU., me asignaron a mi primera especialización: “Cyber Insurance”.

En general los underwriters de seguros especiales evalúan el riesgo y la exposición de clientes potenciales. Deciden cuanta cobertura debe recibir el cliente, cuanto se debe pagar por ella y si se acepta el cliente como riesgo o no. El proceso de underwriting intenta medir la exposición al riesgo y determinar la prima que se debe cobrar para asegurar ese riesgo. La función del underwriter es proteger el libro de negocios de la compañía de los riesgos que cree que generarán pérdidas.

Decidí combinar mi master con mi profesión para presentar el seguro cibernético y intentar resolver un problema común en el proceso de underwriting de un riesgo cibernético, con una simple herramienta que puede ayudar en la gestión de expectativas y de tiempo.

INTRODUCCIÓN DEL TEMA

¿QUÉ ES LA SEGURIDAD CIBERNÉTICA?

Al inicio, es importante entender que significa Cyber. Para empezar, el Internet de las cosas (IoT = “Internet of Things”), junto con la digitalización mundial, son ampliamente considerados como cambios radicales en la evolución de las tecnologías y marcan el inicio de la cuarta revolución. Aunque a menudo se hace referencia en términos de dispositivos de consumo y “smartphones”, no se trata de una sola tecnología independiente. No se puede hablar del IoT o la digitalización como "una cosa", sino “muchas cosas" diferentes conectadas por una red. De hecho, ambos involucran una amplia gama de áreas de aplicación que se extienden mucho más allá del hogar o el día a día, dentro de la infraestructura crítica y el comercio global. Cyber es como el entorno virtual, en el cual todas estas tecnologías se desarrollan y forman. Eso también atrae problemas que exponen empresas a ataques digitales, los cuales se pueden clasificar como riesgos cibernéticos.

La ciberseguridad es la práctica de proteger sistemas, redes y programas de dichos ataques digitales. Estos ataques cibernéticos generalmente tienen como objetivo acceder, cambiar o destruir información confidencial; extorsionar a los usuarios con dinero; o interrumpir los procesos comerciales normales. La implementación de medidas efectivas de ciberseguridad es particularmente desafiante hoy porque hay más dispositivos que personas, y los atacantes se están volviendo más innovadores. Un enfoque exitoso de ciberseguridad tiene múltiples capas de protección repartidas en las computadoras, redes, programas o datos que uno pretende mantener a salvo. En una organización, las personas, los procesos y la tecnología deben complementarse entre sí para crear una defensa efectiva contra los ciberataques.

En un mundo tan conectado como hoy, todos se benefician de los programas avanzados de defensa cibernética. Un ataque de ciberseguridad puede resultar en todo, desde interrupción de negocios, intentos de extorsión, hasta la pérdida o el robo de datos importantes, como información sensible sobre clientes. Plantas de energía, hospitales y compañías de servicios financieros, todos dependen de infraestructura crítica expuesta a dichos ataques. Proteger estas y otras organizaciones del riesgo cibernético es esencial para mantener nuestra sociedad en funcionamiento.

Sin embargo, no es posible protegerse al 100% de un ataque, y normalmente, si es un incidente significante, resulta en una perdida monetaria relativamente grande para las empresas afectadas. Por eso existe un "Cyber Insurance" o seguro cibernético, que da una cobertura extra encima de la defensa cibernética establecida en la organización. Así, los negocios pueden continuar con el mínimo peligro posible.

TENDENCIA ALCISTA DE LA DEMANDA DE SEGUROS CIBERNÉTICOS

El riesgo cibernético es una preocupación creciente para las instituciones, las personas y los mercados financieros. En menos de cinco años, ha subido a las primeras posiciones [5] en la lista de riesgos globales para las empresas. Además, los ciberataques a gran escala ocupan el sexto lugar en la lista de riesgos con mayor probabilidad de ocurrir en los próximos 10 años[5]. Se espera que el creciente número de incidentes cibernéticos, la continua transformación digital y las nuevas iniciativas reguladoras en la Unión Europea generen conciencia y aumenten la demanda de seguros cibernéticos. Las aseguradoras de los EE.UU. empezaron a ofrecer pólizas Cyber en 2010 con poco conocimiento sobre como se evalúa ese riesgo realmente. Cuatro años después, las instituciones europeas empezaron también y hasta 2016 el producto había llegado a todos los mercados financieros del mundo. Se estima una subida exponencial en primas de seguros cibernéticos, por su demanda y peculiaridad de riesgo. Aunque una empresa hace todo lo que se requiere para evitar un ciberataque, puede ocurrir una perdida por un incidente imprevisto, por este motivo las pólizas cuestan y costaran mas que otros productos comparables. Analistas y consultores de Advisen, Allianz y Betterley pronostican hasta USD 20 mil millones de primas por seguros cibernéticos en 2025, que seria un crecimiento de mas del 400% en 5 años o un crecimiento anual de 100%. Datos adicionales que soportan la tendencia alcista es el aumento global de IoT, como demostrado en un estudio de Ericsson en 2017. Se estima que hasta 2025 habrá un IoT instalado globalmente en valor de aproximadamente USD 75 mil millones. Según Tom Bold de Lloyd's, la industria de los seguros cibernéticos está mostrando una innovación real y demuestra la capacidad de las aseguradoras para desarrollar pólizas que cubran riesgos modernos y complejos. Debido a la creciente importancia de esta clase de riesgo, los datos de exposición estandarizados de calidad son críticos para mayores niveles de cobertura de seguro y un mejor modelo de riesgo. En cuanto a las condiciones, el informe Betterley de 2017 demuestra, que las primas han crecido, los asegurados eligen límites más altos y seleccionan tipos adicionales de coberturas cibernéticas. Aon, uno de los brokers de seguros mas grandes dice, que antes se vendía1,2 pólizas por cada 10 consultas; desde ataques digitales recientes son 4,2 por cada 10 consultas.

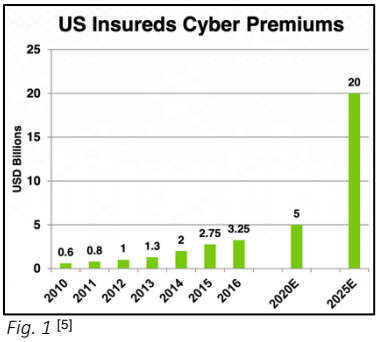


Fig. 1 [5]

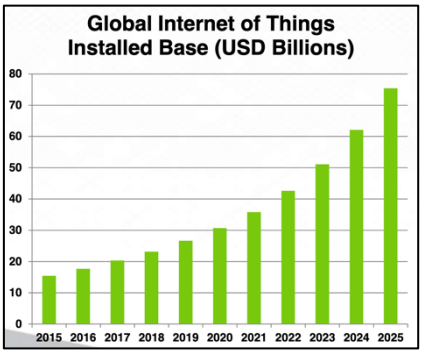


Fig. 2 [5]

¿QUÉ TIPOS DE AMENAZAS EXISTEN PRINCIPALMENTE?

Una empresa puede tener datos de clientes, información de empleados y posiblemente diseños detallados de productos. Es probable que estos sean de interés para los delincuentes. Una conciencia y una comprensión básica de las amenazas planteadas en un mundo cibernético ayudarán a proteger sus activos digitales, propiedad intelectual y su negocio. Entre todos los métodos que existen para realizar un ataque cibernético, hay 5 tipos destacados que provocan la gran mayoría de las perdidas globales.

1. Ransomware
   Esta es una forma de malware (software malicioso) que intenta cifrar (codificar) sus datos y luego extorsionar un rescate para liberar un código de desbloqueo. La mayoría del ransomware se entrega a través de correos electrónicos maliciosos

2. Suplantación de identidad
   La suplantación de identidad, o phishing, es un intento de obtener información confidencial mientras se hace pasar por un contacto confiable, por ejemplo, un banco o un servicio en línea. La suplantación precisa de identidad (Spear Phishing) es un intento muy específico de obtener información de un individuo. Los correos electrónicos de phishing pueden parecer completamente convincentes, a menudo con una redacción impecable y logotipos genuinos. Existe una forma de spear phishing, donde un correo electrónico falso de un CEO aplica presión sobre un CFO para que realice un pago urgente, esto se conoce como Whaling.

3. Data Breach
   Si bien la seguridad cibernética en la oficina puede parecer un desafío, es esencial comprender que la seguridad se extiende mucho más allá de la oficina en estos días. El uso de teléfonos inteligentes y tabletas se ha generalizado. La naturaleza ubicua y barata de los dispositivos de almacenamiento portátiles los convierte en una herramienta útil para la copia de seguridad y el transporte de datos. Estas características significan que también son un objetivo para los ladrones de datos.

4. Hackear y interrupción de negocio
   Obtener acceso a los sistemas de TI desde fuera de una organización aún ofrece opciones enriquecedoras para los delincuentes. Tradicionalmente, han intentado obtener acceso a la información de la cuenta bancaria o las bases de datos de tarjetas de crédito. Sin embargo, la propiedad intelectual es otra fuente de valor. El uso de la ingeniería social, engañando al personal para que revele nombres de usuario y contraseñas, sigue siendo una amenaza. Además, se puede provocar una interrupción total de negocios en un sistema hackeado, voluntariamente e involuntariamente.

5. Amenaza interna
   Si una organización emplea personal (a tiempo completo o como contratistas), existe la posibilidad de que puedan filtrar datos por error o maliciosamente. El daño potencial de una fuga de documentos no puede subestimarse.

Iran, 2010

En septiembre de 2010, los expertos en Irán y los especialistas en seguridad informática estaban cada vez más convencidos de que un virus estaba destinado a sabotear las instalaciones de enriquecimiento de uranio en Natanz, Iran donde la capacidad operativa de la centrífuga se había reducido en el último año por un 30%. Los problemas eran causados por Stuxnet, un gusano informático malicioso. Apunta a los sistemas de control de supervisión y adquisición de datos (SCADA) y se cree que es responsable de causar daños sustanciales al programa nuclear de Irán. Aunque ninguno de los países ha admitido abiertamente su responsabilidad, se entiende ampliamente que el gusano es un arma cibernética construida conjuntamente por Estados Unidos e Israel. En total, este ataque cibernético destruyó 3 años del desarrollo programa nuclear del gobierno de Iran.

Sony, 2014

A fines de noviembre de 2014, Sony Pictures Entertainment fue pirateado por un grupo que se hacía llamar Guardianes de la Paz. Los piratas informáticos, que se cree que están trabajando al menos en cierta conexión con Corea del Norte, robaron grandes cantidades de información de la red de Sony. Rumores suponen que el motivo del ataque fue la película “The Interview”, una comedia, producida por Sony, sobre un par de periodistas, interpretados por Seth Rogen y James Franco, quienes lograron una entrevista con el líder norcoreano Kim Jong Un.

Los atacantes tomaron varios terabytes de datos privados, eliminaron las copias originales de las computadoras Sony y dejaron mensajes que amenazaban con divulgar la información si Sony no cumplía con las demandas de los hackers. En el transcurso de varias semanas, los piratas informáticos publicaron varias oleadas de archivos robados. Los hackers publicaron cinco películas de Sony (cuatro inéditas) y intercambios de archivos. También filtraron miles de documentos confidenciales, desde correspondencia privada entre ejecutivos hasta datos de sueldos y desempeño de los empleados. Se provocó un data breach de 77 millones de cuentas usuarios, incluyendo información sensible financiera, y una interrupción de negocios de 23 días. Las secuelas incluyen una disminución del precio de la acción del 8%, un costo de gestionar el incidente de USD 170 millones y costos de liquidación para una denuncia colectiva. En total, el ciberataque provocó una perdida de USD 2 mil millones. [6]

ESTRUCTURA DE UN SEGURO CIBERNÉTICO CORPORATIVO

Un informe de la EIOPA del 2018 se basa en las respuestas de 13 grupos de seguros con sede en Suiza, Francia, Italia, Alemania y el Reino Unido a un conjunto de 14 preguntas cualitativas para resumir las perdidas cubiertas normalmente en una póliza cibernética. La muestra se seleccionó en función de la experiencia y las exposiciones actuales en seguros cibernéticos y consta de ocho aseguradoras y cinco reaseguradoras. Generalmente se puede decir, que el objetivo de un seguro cibernético es únicamente cubrir las perdidas directamente ocurridas por un incidente de ciberseguridad y la recuperación de del estado original de la infraestructura. Se intenta evitar cualquier labilidad relacionada con gastos ocurridos después del ataque, solo indirectamente provocados por el incidente.

El seguro cibernético se puede ofrecer como un producto independiente y como una cobertura adicional para las líneas de negocios tradicionales. Puede incluir cobertura tanto para responsabilidades de primeros como de terceros (proveedores de servicios, etc.).
Todos los grupos en la muestra ofrecen cobertura para pasivos de terceros y / o una combinación de ambos. Los tipos más comunes de cobertura ofrecidos son la interrupción del negocio (BI) y la restauración de datos. La mayoría de las empresas de seguros también proporcionan cobertura de extorsión cibernética y apoyo legal, aunque en menor medida. Cinco empresas de la muestra también ofrecen cobertura por cuestiones de reputación.
Típicamente, este tipo de cobertura contiene la pérdida de ganancias netas directamente relacionadas con un ataque cibernético, similar a una cobertura de interrupción de negocios, pero también proporciona soporte adicional para el costo de contratar consultores de relaciones públicas para ayudar a gestionar la percepción pública del asegurado después de un incidente cibernético. [10]

- Interrupción de negocio
  La cobertura de una interrupción de negocios es un tipo de seguro que cubre la pérdida de ingresos que una empresa sufre después de un incidente cibernético. La pérdida de ingresos cubierta puede deberse al cierre de la instalación comercial relacionada con el desastre o al proceso de reconstrucción después de un desastre.

- Data Breach
  Un data breach es un tipo de cobertura comprada por las organizaciones para proteger los intereses financieros en caso de pérdida de datos. Las violaciones de datos se producen por varias razones, que incluyen piratería y procedimientos de ciberseguridad deficientes.

- Extorsión cibernética y otros gastos legales
  La extorsión cibernética puede adoptar diversas formas, pero el ransomware, con mucho, es la variante más común. La cobertura de extorsión cibernética se creó específicamente para cubrir las pérdidas en las que incurre un incidente de extorsión cibernética y, por lo tanto, puede ofrecer la mejor oportunidad para que un asegurado obtenga una determinación de cobertura favorable de su asegurador. Además, también se cubren posibles gastos legales directamente relacionados con el incidente.

- Costos de defensa/sanciones
  Por ultimo, como en casi cada seguro corporativo, hay una cobertura de costos de defensa o sanciones. Estos costos de se refieren a todos los costos de defenderse contra una denuncia. Estos gastos incluyen el costo de contratar a un abogado, honorarios judiciales, investigaciones, recopilación de hechos, presentación de documentos legales y otros costos relacionados.

Por ultimo, es importante explicar la estructura de capacidades provistos de las aseguradoras a través del enfoque de exceso de pérdida. La construcción de un programa de cobertura de seguro utilizando capas implica una serie de aseguradoras que proveen una definida cantidad monetaria de cobertura, cada una en exceso de los límites inferiores de otras aseguradoras. La cobertura de responsabilidad general se estructura con frecuencia de esta manera, por lo que una serie de aseguradoras proporcionan cobertura en varios niveles, sobre una base de exceso de pérdida. La aseguradora con capacidad en la primera capa, que se llama “Primary”, tiene una exposición directa e inmediata en el caso de un incidente, una vez el daño ocurrido supera el deducible. Además, la aseguradora en el Primary también define el texto o los detalles de la póliza y da la base para la fijación de primas en el resto de la estructura. Por lo tanto, cuanto mas baja una capa esta, mas prima se cobra por la cobertura y mas importancia tiene en el programa.

INTRODUCCIÓN DEL TRABAJO

ENFOQUE DEL TRABAJO

Este trabajo se realizó para ocupar un nicho relacionado con el proceso de underwriting de riesgos cibernéticos. Por la novedad del producto y una falta general de educación sobre ello, aun existen muchas ideas equivocadas sobre el tema. Especialmente los corredores de seguros y sus clientes tienen expectativas desproporcionadas del mercado y no entienden bien, que factores impactan un riesgo cibernético y como se evalúan. Una dificultad específica reconocida es la falta de similitud en el lenguaje de evaluación de riesgos, que se hace evidente en varios aspectos, desde la cobertura hasta los cuestionarios para los clientes de las aseguradoras diferentes. Por su exposición amplia, un seguro cibernético además requiere una valoración bastante técnica, que a veces no se entiende en el mercado, porque el proceso es mas informático que financiero. Otro punto problemático seria la dependencia de terceros para conseguir la información relevante que sirve para la valoración del riesgo. En total hay un relativamente largo proceso entre la presentación de una empresa a través de un corredor y la primera indicación de precio para una póliza correspondiente del asegurador. Para incluir una organización en el libro de negocios y ofrecerle una póliza, hay 2 puntos clave para verificar antes:

Análisis del apetito al riesgo
Primero, la aseguradora quiere ver si vale la pena aceptar el riesgo. Esta parte del proceso de underwriting incluye todo el análisis técnico de las instalaciones de TI, la seguridad cibernética establecida y la creación del texto y las limitaciones de la póliza. Este proceso es vital para determinar si se acepta o rechaza la solicitud.

Análisis del precio de la póliza
Cuando ya se haya determinado que se acepta la solicitud, viene la parte de la fijación de precio que depende parcialmente de la evaluación técnica, pero también sigue otras pautas. Hay limitaciones que varían según las condiciones del mercado o las primas de la competencia.

El análisis de precio se puede homogenizar mejor, enfocándose en factores de riesgo tanto como variables mensurables y comparables que aumentarían o disminuirían la prima. El análisis del apetito, en cambio, es un proceso muy especifico y casi siempre diferente. Una vez que se acepte la solicitud y se acabe el análisis de apetito, se supone que la fijación de la prima sigue una linealidad, dependiendo de determinados factores claves. Dado eso, el estudio se enfocaba en la segunda parte de evaluación, con el objetivo de mejorar la fluidez de comunicación entre partidos y generalizar la valoración de primas.

OBJETIVO DEL TRABAJO

El objetivo principal de este trabajo era la creación de una herramienta para dar indicaciones precisas de primas de pólizas cibernéticas y al mismo momento gestionar mejor las expectativas de cada partido involucrado mientras se ahorra tiempo. Esta herramienta se limitaba a pólizas para instituciones financieras en Europa, para precisar la muestra sobre la cual se creó el modelo. El producto final debe dar una indicación de una prima basada en factores clave predeterminados que se eligieron para definir el nivel de riesgo de una empresa en forma de una calculadora. El resultado debería intentar a simplificar y normalizar las primas cibernéticas de las instituciones financieras mientras el underwriter se independiza de la necesidad de conseguir toda la información del bróker. Por eso, hizo falta primero encontrar variables que definen bien la exposición cibernética de una empresa y que se dejen derivar de información inicial fácilmente accesible. El enfoque al sector financiero viene por dos motivos:
Uno es la motivación fuerte de atacar un banco o una agencia de seguros, por los datos sensibles que normalmente guardan estas empresas y el beneficio que se puede generar con ellos.

El otro motivo es la amplia información accesible para realizar el estudio adecuadamente y crear un modelo que de resultados confiables. Por ultimo, como se trataba de un trabajo de master en banca y finanzas, seria un motivo adicional de dedicar y centrar la investigación del sector financiero.

La idea de aplicación sería, que el underwriter pueda dar una prima normalizada según informaciones iniciales sobre la exposición cibernética de una institución, sin tener que acabar el proceso de análisis técnico del riesgo. Así, los corredores ya saben la posible dimensión de primas en antelación y pueden crear la estructura del programa de seguro, mientras las aseguradoras tienen mas tiempo para evaluar la compañía. Finalmente, también se pueden aplicar ajustes a la prima indicada al principio si necesario. También, se lograría educar el mercado y homogenizar el enfoque, como fue el caso con otros productos de seguro.

LITERATURA

I. Separating the Truths from the Myths in Cybersecuri by Ponemon Institute, 2019
El Instituto Ponemon, con el patrocinio de BMC, realizó el estudio sobre Separando las Verdades de los Mitos en Ciberseguridad para comprender mejor los mitos de seguridad que pueden ser barreras para una función de seguridad de TI más efectiva y para determinar las verdades que deben considerarse importante para la postura de seguridad general. En el contexto de esta encuesta, las verdades de seguridad cibernética son basado en la experiencia real de los participantes en esta investigación. En contraste, los mitos de ciberseguridad se basan en sus percepciones, creencias y sensaciones viscerales. Más de 1.300 profesionales de TI y seguridad de TI en Norteamérica (NA), Reino Unido (UK) y EMEA que tienen varios roles en operaciones de TI y seguridad fueron encuestados. Todos los encuestados conocen las estrategias de seguridad de TI de sus organizaciones. El Ponemon Institute es imprescindible para presentar este estudio el tema relacionado.

II. Cost of a Data Breach by IBM Security, 2019
IBM Security and Ponemon Institute lanzó el Informe de costo de una violación de datos de 2019. Basado en entrevistas en profundidad con más de 500 empresas en todo el mundo que experimentaron una violación de datos entre julio de 2018 y abril de 2019, el análisis en este estudio de investigación toma en cuenta cientos de factores de costo, desde actividades legales, regulatorias y técnicas, hasta pérdidas de valor de marca, rotación de clientes y la pérdida de productividad de los empleados. El informe da una amplia idea y recerca que sirve para monitorizar una perdida de datos, que es crucial para el proceso de underwriting y ha revolucionado la evaluación de este tipo de riesgo.

III. Cyence Report
Guidewire Software Inc., comúnmente Guidewire, es un editor de software con sede en San Mateo, California. Ofrece una plataforma industrial para compañías de seguros de propiedad y accidentes (P&C) en los EE.UU. y en todo el mundo. En los últimos años, también se especializaron mas en Cyber. Cyence es parte del proceso de modelado económico que combina lo mejor de la experiencia de Marsh (el mejor corredor de Cyber en el mercado), así como asociaciones en todo el mundo para ayudar a impulsar modelos económicos superiores para que los clientes entiendan su entorno particular de riesgo cibernético. El Cyence report en si, se puede generar para cualquier empresa guardada en la base de datos de Guidewire y era una de las bases de recursos principales para realizar este trabajo.

METODOLOGÍA

Los datos utilizados para este estudio incluyen datos primarios y datos secundarios. Para crear la herramienta requerida, fue necesario derivar y homogeneizar los datos iniciales y aplicar un modelo de regresión lineal sobre ellos. Entonces, fue posible crear una ecuación que estima una prima basada en varias variables. Este proceso se puede dividir en cinco partes:

1. Colección de información secundaria – la cartera/muestra
2. Colección de información primaria – la encuesta
3. Derivación de variables
4. Correlaciones
5. Creación del sujeto de estudio - la matriz

MODELOS DE DATOS

INFORMACIÓN SECUNDARIA – LA CARTERA

El primer paso para crear una herramienta que permite evaluar una prima homogenizada de una póliza cibernética es la búsqueda por una muestra fiable de instituciones financieras en Europa. Dentro de los servicios financieros existen varios sectores, por lo tanto, para empezar, se definieron dos sectores en especifico que se incluirán en la muestra:

- Servicios Bancarios y/o Gestoras de Inversión (Banking Services and/or Asset Managers)
- Aseguradoras y/o Agencias de Seguros (Insurance Carriers, Agents and/or Brokers)

COUNTRIES	GDP	GDP YoY	GDP QoQ	Interest rate	Inflation rate	Jobless rate
Euro Area	14000	-3.10%	-3.60%	0.00%	0.10%	7.30%
Germany	4040	-2.30%	-2.20%	0.00%	0.60%	3.50%
United Kingdom	2910	-1.60%	-2.00%	0.10%	0.50%	3.90%
France	2890	-5.00%	-5.30%	0.00%	0.40%	7.80%
Italy	2030	-5.40%	-5.30%	0.00%	-0.20%	6.30%
Russia	1750	1.60%	0.60%	4.50%	3.00%	6.10%
Spain	1460	-4.10%	-5.20%	0.00%	-0.90%	14.41%
Netherlands	951	-0.20%	-1.50%	0.00%	1.20%	3.60%
Turkey	740	4.50%	0.60%	8.25%	11.39%	13.20%
Switzerland	715	-1.30%	-2.60%	-0.75%	-1.30%	3.40%
Poland	605	2.00%	-0.40%	0.10%	2.90%	6.00%
Sweden	575	0.40%	0.10%	0.00%	0.00%	9.00%
Belgium	532	-2.50%	-3.60%	0.00%	0.48%	5.60%
Austria	459	-2.90%	-2.60%	0.00%	0.70%	11.50%

Fig. 3 tradingeconomics.com

En cuanto al enfoque geográfico, la búsqueda principal se orientaba a países desarrollados con mayor fuerza económica y el PIB mas grande de Europa, también considerando aquellos que tienen mucha importancia especialmente por su sector financiero. Siguiendo estas pautas, los países mas destacados son El Reino Unido, Alemania, Francia, España y Italia. Un resultado poco sorprendente, teniendo en cuenta que las cuatro economías que utilizan la moneda europea generan 74% del PIB de la Zona Euro y El Reino Unido es famoso como capital financiera de Europa. Sin embargo, por su gran relevancia e importante papel en el mundo financiero, era imprescindible incluir Suiza, dado que unas de las instituciones financieras mas grandes, prestigiosas y exitosas del mundo tienen su sede y origen ahí.

Según el estándar internacional, una muestra de recerca considerable debe tener al menos n=30, entonces se decidió definir una cartera de n=40 instituciones financieras, partiéndolas entre 20 Bancos y/o Gestoras de Inversión y 20 Aseguradoras y/o Agencias de Seguros.
Para realmente considerar información relevante y crear una muestra significativa, hacia falta implementar restricciones adicionales. Por eso, solo se consideraban empresas "large-cap" con una capitalización mínima de USD 2 mil millones y ganancias de al menos USD 6 mil millones que cotizan en bolsa, así, se hace mucho mas fácil conseguir los datos necesarios de recursos fiables y coherentes. En comparación con el índice S&P 500 del sector financiero, cuya cartera en total generaría ganancias de USD 9.693 mil millones, la cartera de este estudio llega a un 16% de tal importe. Esta proporción da enfoque adicional a la notable influencia que deben tener las instituciones consideradas en la muestra al sector financiero europeo.

	Real Revenue	
Portfolio	$ 1.502.803.000.000,00	16%
S&P 500 FI Sector	$ 9.693.961.000.000,00	

Table 1 capitaliq.com

Location	# of companies	%
United Kingdom	8	20%
Switzerland	7	18%
France	6	15%
Germany	6	15%
Spain	4	10%
Italy	4	10%
Netherlands	2	5%
Sweden	1	3%
Austria	1	3%
Denmark	1	3%

Table 2

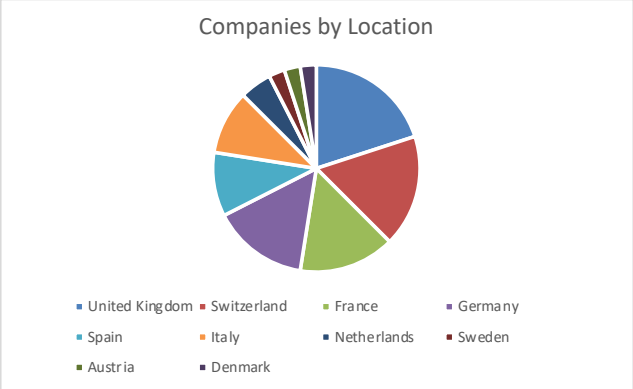


Fig. 4

Como resultado, se creó una cartera adecuada, incluyendo las aseguradoras y los bancos mas grandes de Europa. El Reino Unido y Suiza, como centros financieros europeos y globales, tienen la presencia mas grande con 38%. Justo después vienen las dos economías mas importantes de la Unión Europea, Alemania y Francia, con un peso común de 30%. Italia y España representan el sur de Europa con 20% y como factor adicional de diversificación se escogieron empresas de Suecia, Dinamarca, Austria y los Países Bajos para los últimos plazos.

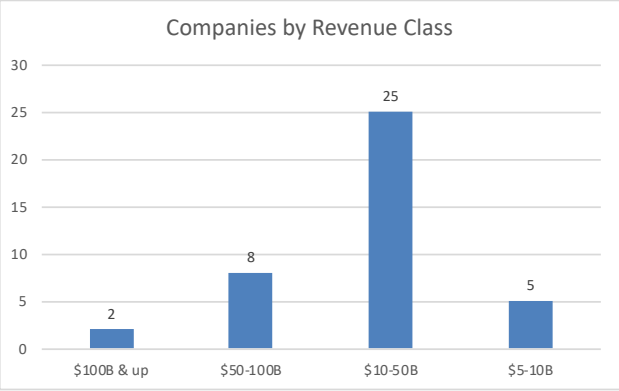


Fig. 5

En cuanto a la distribución por tamaño, se determinaron las ganancias como factor principal de comparación. Para clasificar mejor las instituciones se definieron 4 categorías:

- $ 5-10 mil millones
- $ 10-50 mil millones
- $ 50-100 mil millones
- $ 100 y mas mil millones

La gran mayoría de las empresas en la muestra (82%) tienen entre USD 10 y 100 mil millones de ganancias, solo siete están por debajo o por encima de este porcentaje.

Insurance Carriers, Agents and/or Brokers		Banking Services and/or Asset Managers	
Aegon N.V.	NL	Banco Bilbao Vizcaya Argentaria, S.A.	ES
Allianz SE	DE	Banco Santander, S.A.	ES
Assicurazioni Generali S.p.A.	IT	Barclays PLC	GB
Aviva PLC	GB	BNP Paribas, S.A.	FR
AXA Group, S.A.	FR	Caixabank, S.A.	ES
Chubb Limited	CH	Commerzbank AG	DE
CNP Assurances	FR	Credit Agricole, S.A.	FR
Mapfre, S.A.	ES	Credit Suisse Group AG	CH
Hannover Rück SE	DE	Danske Bank A/S	DK
Helvetia Holding AG	CH	Deutsche Bank AG	DE
Legal & General Assurance Society Ltd	GB	HSBC Holdings PLC	GB
Munich Re	DE	ING Groep N.V.	NL
Prudential PLC	GB	Intesa Sanpaolo S.p.A.	IT
Scor SE	FR	Lloyds Banking Group PLC	GB
Swiss Life Holding AG	CH	Nordea Bank AB	SE
Swiss Re AG	CH	Societe Generale Group	FR
Talanx AG	DE	Standard Chartered PLC	GB
Unipol Gruppo S.p.A.	IT	The Royal Bank Of Scotland PLC	GB
Vienna Insurance Group AG	AT	UBS Group AG	CH
Zurich Insurance Group AG	CH	UniCredit S.p.A.	IT

Fig. 6

La tabla anterior muestra la totalidad de empresas consideradas en la muestra. Para terminar el primer paso y realizar los cálculos de variables, hubo que rellenar primero la base de datos con la información bruta necesaria. La base de datos final consiste de las siguientes cinco informaciones sobre cada una de las 40 instituciones financieras en la cartera:

Market Cap	Real Revenue	Estimated Record Count	Employee Count	Avg. annual loss (AAL)

Table 3

- Market Cap
  La capitalización de mercado es un indicador para determinar la cuota de mercado.
- Real Revenue
  Las ganancias "reales" son básicamente un indicador para la rentabilidad de las empresas.
- Estimated Record Count
  El recuento estimado de datos se refiere a los sets de datos sensibles que la empresa guarda.
- Employee Count
  El recuento de empleados es un indicador para entender la dimensión y presencia que tiene la empresa.
- Avg. annual loss (AAL)
  El promedio anual de la pérdida representa la cuantidad de dinero perdido por incidentes cibernéticas.

INFORMACIÓN PRIMARIA – LA ENCUESTA

El segundo paso era la asignación de la prima / millón de seguro más adecuada y realista posible a cada una de las empresas de la cartera. Conseguir las primas oficiales es casi imposible, dado el alto nivel de confidencialidad de esta información. Además, tampoco hay una sola base de datos que contiene toda esta información, se debería contactar con cada empresa directamente para conseguirla. Entonces, para realizar el análisis adecuado se necesitaron primas homogenizadas, pero realistas. Por lo tanto, se preparó una encuesta abierta, con el objetivo de conseguir una indicación razonable para cada una de las instituciones financieras. En colaboración con 12 underwriters profesionales, todos especializados en seguros cibernéticos, se podía crear una estimación cercana a la realidad de cuanto debería costar el primer millón de una póliza cibernética. Las instrucciones eran las siguientes:

- Dar una indicación (prima) considerando la información cruda en nuestra bbdd
- Indicación es sujeto al hipotético resultado positivo de la evaluación técnica del riesgo
- Incluir experiencias reales en el razonamiento de la evaluación
- Se considera un mercado neutro
- prima / millón de seguro
- No se consideran comisiones, diferencias geográficas o el texto de la póliza
- El seguro cubre primeros y terceros
    - Interrupción del negocio
    - Data Breach
    - Extorsión cibernética y otros gastos legales directamente relacionados con el incidente
    - Costos de defensa/sanciones
- El deducible de la prima depende de la categoría de tamaño:

Rev. Class	Retention (Mn)
$5-10B	$ 1,50
$10-50B	$ 2,00
$50-100B	$ 3,50
$100B & up	$ 5,00

"Rev. Class" es categoría de tamaño
"Retention (Mn)" es deducible en millones

Table 4

Company Name	UW 1	UW 2	UW 3	UW 4	UW 5	UW 6	UW 7	UW 8	UW 9	UW 10	UW 11	UW 12	UW AVG
HSBC Holdings PLC													100%
Allianz SE													76%
AXA Group, S.A.													67%
Banco Santander, S.A.													66%
Deutsche Bank AG													63%
Barclays PLC													55%
BNP Paribas, S.A.													52%
Lloyds Banking Group PLC													48%
Commerzbank AG													47%
Intesa Sanpaolo S.p.A.													45%
Zurich Insurance Group AG													45%
UBS Group AG													43%
Banco Bilbao Vizcaya Argentaria, S.A.													41%
Societe Generale Group													41%
Standard Chartered PLC													41%
Prudential PLC													40%
The Royal Bank Of Scotland PLC													40%
Chubb Limited													40%
Munich Re													39%
ING Groep N.V.													37%
Credit Suisse Group AG													34%
Aviva PLC													34%
UniCredit S.p.A.													34%
Aegon N.V.													34%
Assicurazioni Generali S.p.A.													33%
Nordea Bank AB													32%
Swiss Re AG													29%
Credit Agricole, S.A.													26%
Caixabank, S.A.													25%
Hannover Rück SE													25%
Legal & General Assurance Society Ltd													23%
Mapfre, S.A.													23%
Swiss Life Holding AG													22%
CNP Assurances													22%
Talanx AG													22%
Danske Bank A/S													21%
Scor SE													20%
Helvetia Holding AG													19%
Unipol Gruppo S.p.A.													18%
Vienna Insurance Group AG													17%

Table 5

Cada uno de los underwriters tiene varios años de experiencia en su profesión y en total eran profesionales de tres aseguradoras diferentes. Todos trabajan en mercados europeos representados en la cartera. En algunos de los casos, los underwriters conocían las pólizas reales de la cartera, por haberlas tramitado, así se permitía una estimación aún más fiable. Aunque la implementación y el análisis de este trabajo se había hecho con valores absolutos, solo se puede publicar la tabla de la encuesta con valores relativos, por temas relacionadas con la confidencialidad de información. Aunque teóricamente solo se trata de una estimación, por la simple información privilegiada y experiencia que tienen los underwriters, los resultados de la encuesta ya se pueden considerar confidenciales por su probable similitud con las primas oficiales. La tabla modificada enseña cuales serían las pólizas mas caras y/o mas baratas en porcentaje sobre el precio máximo. Con esta visualización se puede demostrar muy adecuadamente como la muestra esta evaluada y como los precios están distribuidos.

Para hacer la regresión lineal, el siguiente paso era definir las variables que deberían determinar el precio de la póliza cibernética. La información bruta inicial de la base de datos tuvo que derivarse y convertirse en valores normalizados y comparables. Para hacerlo, se aplicaron cálculos típicos de evaluación para riesgos cibernéticos y se ponderaron con factores cruciales del Informe Cyence.

DERIVACIÓN DE VARIABLES

Market Cap

$$MC = MC$$

MC: capitalización de mercado

Fig. 7

Además de un indicador de cuota de mercado, la capitalización de mercado es la base utilizada del underwriter cuando se trata de determinar un tamaño de referencia para una empresa.

Estimated Hourly Loss

$$EHL = \frac{RR * r}{(d*h)}$$

EHL: pérdida por hora estimada
RR: ganancias reales
r: ratio de susceptibilidad de Cyence
d: días hábiles (253)
h: horas hábiles por día (8)

Fig. 8

La pérdida por hora estimada se deriva de los ingresos reales de la empresa divididos entre días hábiles y horas hábiles por día. Posteriormente, este valor fue ponderado por la ratio de susceptibilidad de Cyence.

Estimated DB Exposure

La exposición estimada de data breach tiene en cuenta el recuento estimado de datos más el recuento de empleados, suponiendo que cada empleado tiene un set de datos en la empresa. El recuento se puede conseguir de dos formas: Una sería recibir los datos reales del cliente o del corredor y la otra sería coger la estimación del informe Cyence. El número conjunto de sets de datos se convierte en valores monetarios y comparables, multiplicándolo con el costo correspondiente de acuerdo con el informe de Ponemon, también teniendo en cuenta el país de origen de cada empresa. Este valor monetario teórico de los datos se pondera con los porcentajes de información crediticia que posee cada empresa y la probabilidad de tener un data breach, ambos proporcionados por el informe Cyence para conseguir la exposición estimada de data breach.

Country	Country ID	Cost of Breach per Data Set
Germany	DE	188
France	FR	169
Italy	IT	152
Great Britain	GB	148
Others*	AT	148
	CH	148
	DK	148
	ES	148
	NL	148
	SE	148

Fig. 9 [2]

$$EDBE = (ERC+EC) * P*c*p$$

EDBE: exposición estimada de data breach
ERC: recuento estimado de datos
EC: recuento de empleados d: días hábiles (253)
P: costo Ponemon
c: porcentaje de información crediticia
p: probabilidad de tener un data breach

Fig. 10

Motivation based on AAL

Para expresar la motivación en unidades monetarias, la pérdida promedia anual se tomó como base y se ponderó con la ratio de motivación de Cyence.

Combined Ratio - Motivation				
Weight	**External Presence (0, 4)**	**Social Media Presence (0, 4)**	**Web Popularity (0, 4)**	**Publicity (0, 4)**
6,25%	0	0	0	0
6,25%	1	1	1	1
6,25%	2	2	2	2
6,25%	3	3	3	3
6,25%	4	4	4	4

Table 6

Adicionalmente se ponderó con una ratio combinada que representa varios factores, cuales aumentarían la motivación de un ataque cibernético. Esta ratio combinada contenía la presencia externa, la presencia en las redes sociales, la popularidad de la pagina web y la publicidad - cada actividad se valoraba de 0 a 4, siendo 0 la puntuación mas baja y 4 la puntuación mas alta. Cada punto individual tiene una ponderación de 6,25%, que significa una puntuación total de 16 (todas las cuatro actividades evaluado con 4) resultaría en una ratio combinada de 100% y entonces aumentaría el valor de la motivación basada en la pérdida promedia anual.

$$M = AAL * m * 6{,}25\% * (e+s+w+p)$$

M: motivación basada en la pérdida promedia anual
AAL: pérdida promedia anual
m: ratio de motivación de Cyence
e: puntuación presencia externa
s: puntuación presencia en las redes sociales
w: puntuación popularidad de la pagina web
p: puntuación publicidad

Fig. 11

CORRELACIONES

Junto con las cuatro variables y el precio estimado de la póliza, fue posible realizar la regresión lineal y crear el modelo que era fundamental para la herramienta de evaluación final. Sin embargo, antes de continuar, era necesario analizar la correlación entre las variables elegidas para deshacerse de factores redundantes. Con cuatro variables se deben considerar los 6 coeficientes que representan las correlaciones entre cada una de ellas. Los coeficientes de correlación cuya magnitud está entre 0,5 y 0,7 indican variables que pueden considerarse moderadamente correlacionadas mientras los coeficientes de correlación cuya magnitud está entre 0,3 y 0,5 indican variables que tienen una baja correlación. En el análisis se observó, que las variables generalmente están poco o sólo moderadamente relacionadas. La pérdida por hora estimada y la exposición estimada de data breach, que son los dos factores más consideradas en riesgos cibernéticos, casi no tienen correlación con un coeficiente de 0,16. Se ve una moderada relación entre la pérdida por hora estimada y la capitalización de mercado porque, sin embargo, existe una tendencia que una empresa con una cuota de mercado grande también genera más ganancias y entonces existe una posible pérdida por hora más grande. No obstante, la relación es suficientemente baja para conservar ambas variables.

factor correlations		
Correlation	**Feature 1**	**Feature 2**
94%	Estimated DB Exposure	Motivation based on AAL
58%	Estimated Hourly Loss	Market Cap
56%	Market Cap	Motivation based on AAL
41%	Estimated DB Exposure	Market Cap
36%	Estimated Hourly Loss	Motivation based on AAL
16%	Estimated DB Exposure	Estimated Hourly Loss

Table 7

Lo mismo pasó con la capitalización del mercado y la motivación. Una empresa con una cuota de mercado grande también es más probable de tener ataques cibernéticos y, como resultado, sufrir pérdidas. La relación también es suficientemente baja para conservar ambas variables. Aunque sorprendentemente se veía que había una relación significativa entre la exposición estimada de data breach y la motivación basada en la pérdida promedia anual, hay un escenario clave de considerar: si una empresa tuviera un recuento de datos muy bajo, pero sufrió una perdida por una interrupción de negocios, u otro incidente que no sea data breach, que provocó perdidas grandes, las dos variables no estarían tan relacionadas. Además, tanto la perdida promedia anual, que es la base de la variable de motivación, como la exposición estimada de data breach son imprescindibles en cuanto a la evaluación de un riesgo cibernético. En conclusión, se decidió conservar los dos también.

Finalmente, el último paso fue crear la ecuación de la prima con un análisis de regresión lineal. La tabla muestra la base de datos final y normalizada que representa la cartera para este estudio.

Company Name	Country	Market Cap	Estimated Hourly Loss	Estimated DB Exposure	Motivation based on AAL	Primary Premium / Mn
HSBC Holdings PLC	GB					100%
Allianz SE	DE					76%
AXA Group, S.A.	FR					67%
Banco Santander, S.A.	ES					66%
Deutsche Bank AG	DE					63%
Barclays PLC	GB					55%
BNP Paribas, S.A.	FR					52%
Lloyds Banking Group PLC	GB					48%
Commerzbank AG	DE					47%
Intesa Sanpaolo S.p.A.	IT					45%
Zurich Insurance Group AG	CH					45%
UBS Group AG	CH					43%
Banco Bilbao Vizcaya Argentaria, S.A.	ES					41%
Societe Generale Group	FR					41%
Standard Chartered PLC	GB					41%
Prudential PLC	GB					40%
The Royal Bank Of Scotland PLC	GB					40%
Chubb Limited	CH					40%
Munich Re	DE					39%
ING Groep N.V.	NL					37%
Credit Suisse Group AG	CH					34%
Aviva PLC	GB					34%
UniCredit S.p.A.	IT					34%
Aegon N.V.	NL					34%
Assicurazioni Generali S.p.A.	IT					33%
Nordea Bank AB	SE					32%
Swiss Re AG	CH					29%
Credit Agricole, S.A.	FR					26%
Caixabank, S.A.	ES					25%
Hannover Rück SE	DE					25%
Legal & General Assurance Society Ltd	GB					23%
Mapfre, S.A.	ES					23%
Swiss Life Holding AG	CH					22%
CNP Assurances	FR					22%
Talanx AG	DE					22%
Danske Bank A/S	DK					21%
Scor SE	FR					20%
Helvetia Holding AG	CH					19%
Unipol Gruppo S.p.A.	IT					18%
Vienna Insurance Group AG	AT					17%

Table 8

Las variables específicas se representan en un mapa de calor, donde los campos verdes tienen valores bajos que disminuirían el precio y los campos rojos tienen valores altos que aumentarían el precio. La prima asignada a cada institución financiera esta representado en números relativos, siguiendo los cálculos anteriormente mencionados. Así, se puede ver con mas claridad cuales factores resultan en que precio. A través de los valores absolutos de esta base de datos se podían calcular los coeficientes de cada variable, que determinan la ponderación que tienen en la evaluación del precio y, por lo tanto, permiten proponer una ecuación para la herramienta. La fórmula considerada para el modelo es la siguiente:

$$Prima = i+(a*MC+b*EHL+c*EDBE+d*M)$$

i: intercepción (precio base)
a: coef. capitalización de mercado
b: coef. pérdida por hora estimada
c: coef. exposición estimada de data breach
d: coef. motivación basada en la pérdida promedia anual
MC: capitalización de mercado
EHL: pérdida por hora estimada
EDBE: exposición estimada de data breach
M: motivación basada en la pérdida promedia anual

Fig. 12

RESULTADO

ECUACIÓN DEL MODELO DE REGRESIÓN LINEAL

El resultado del análisis de regresión lineal dió la intersección, que es el precio mínimo el modelo asume como prima, y los cuatro coeficientes a, b, c y d. El precio mínimo se debe interpretar como la prima básica de una póliza cibernética, considerando que todos los factores determinados para influenciarla son iguales a cero. Por lo tanto, según este modelo, la prima no puede valer menos que USD 7.986,46. Los coeficientes ponderan las variables de acuerdo con la prima correspondiente. Por el contrario, si se dispone de las variables y se requiere evaluar la prima, los coeficientes junto con la intersección finalizan la ecuación del modelo de regresión lineal para evaluarla:

linear regression model	
coef	**name**
7986,46	intercept
0,000000192	Market Cap
0,000129822	Estimated Hourly Loss
0,000001807	Estimated DB Exposure
0,001026448	Motivation based on AAL

Table 9

$$Prima = 7986{,}46 + (1{,}92*10^{-7}*MC + 1{,}29*10^{-4}*EHL + 1{,}80*10^{-6}*EDBE + 1{,}02*10^{-3}*M)$$

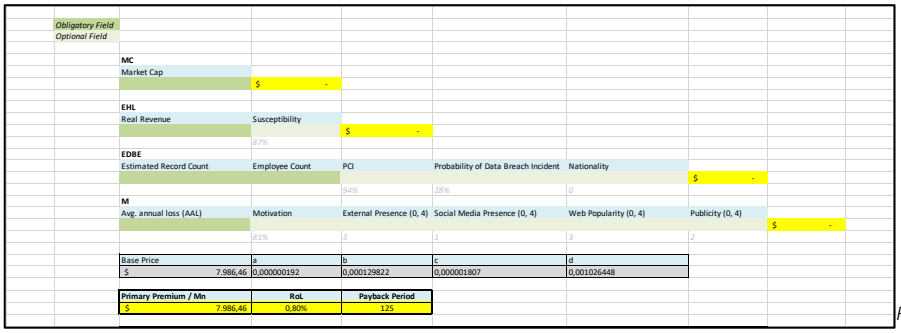
MC: capitalización de mercado
EHL: pérdida por hora estimada
EDBE: exposición estimada de data breach
M: motivación basada en la pérdida promedia anual

Fig. 13

La fórmula forma parte del objetivo de este trabajo y sirve como la base para la herramienta de estimación presentado en la próxima parte. Antes, es importante mencionar, que la exactitud y la fidelidad de los resultados de la ecuación creada con la regresión lineal se limita a escenarios restringidos por las pautas consideradas durante todo el estudio.

HERRAMIENTA DE EVALUACIÓN

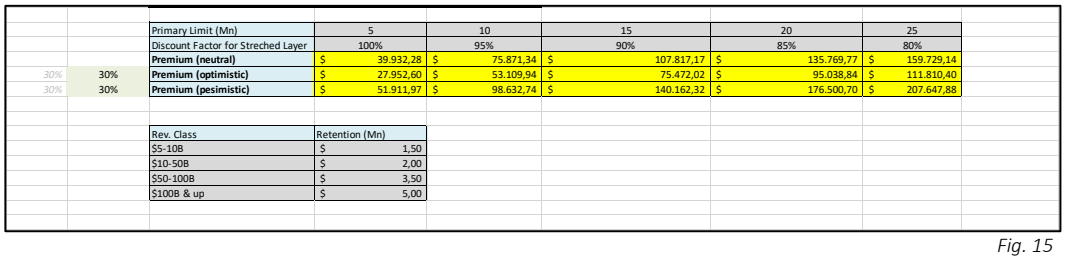
Como resultado final y producto terminado del trabajo, se puede presentar la herramienta de evaluación para determinar una indicación relevante de una prima para una póliza de un seguro cibernético. La calculadora procesa los datos introducidos con las formulas de acuerdo con los conceptos anteriormente explicados. Aplicando la ecuación del modelo de regresión lineal, con las variables calculadas se determina una prima / millón de seguro. También se calcula la ratio RoL, que básicamente es la prima dividida entre la cantidad de dinero previsto por la aseguradora, y el periodo de recuperación de dinero, que son los años que se necesitarían cobrar la prima para recuperar una hipotética perdida entera en el caso de un incidente. Para cumplir con el objetivo de simplicidad, pero eficiencia con menos dependencia de los proveedores de información, la herramienta ya puede dar resultados adecuados con solo cinco datos obligatorios que son: la capitalización de mercado, las ganancias reales, el recuento estimado de datos, el recuento de los empleados y la pérdida promedia anual.



Obligatory Field							
Optional Field							
MC							
Market Cap							
	$ -						
EHL							
Real Revenue	Susceptibility						
		$ -					
	87%						
EDBE							
Estimated Record Count	Employee Count	PCI	Probability of Data Breach Incident	Nationality			
					$ -		
		94%	28%	0			
M							
Avg. annual loss (AAL)	Motivation	External Presence (0, 4)	Social Media Presence (0, 4)	Web Popularity (0, 4)	Publicity (0, 4)		
						$ -	
	81%	3	2	3	2		
Base Price	a	b	c	d			
$ 7.986,46	0,000000192	0,000129822	0,000001807	0,001026448			
Primary Premium / Mn	RoL	Payback Period					
$ 7.986,46	0,80%	125					

Fig. 14

Toda esta información es accesible para un underwriter a través del cliente, el corredor o información publicada. Los datos opcionales pueden ser los valores predefinidos, que son los promedios de la muestra. En el mejor escenario posible, todos los datos obligatorios están entregados por el cliente o su corredor directamente y los datos opcionales son accesibles en el informe Cyence y/o el informe anual de la institución financiera.



		Primary Limit (Mn)	5	10	15	20	25
		Discount Factor for Streched Layer	100%	95%	90%	85%	80%
		Premium (neutral)	$ 39.932,28	$ 75.871,34	$ 107.817,17	$ 135.769,77	$ 159.729,14
30%	30%	**Premium (optimistic)**	$ 27.952,60	$ 53.109,94	$ 75.472,02	$ 95.038,84	$ 111.810,40
30%	30%	**Premium (pesimistic)**	$ 51.911,97	$ 98.632,74	$ 140.162,32	$ 176.500,70	$ 207.647,88

Rev. Class	Retention (Mn)
$5-10B	$ 1,50
$10-50B	$ 2,00
$50-100B	$ 3,50
$100B & up	$ 5,00

Fig. 15

Además, la herramienta también ofrece diferentes primas para diferentes escenarios. Hay dos factores principales para estos escenarios: la capacidad del seguro provisto y las condiciones del mercado. En cuanto a las capacidades, hay resultados alternativos para 5 millones, 10 millones, 15 millones, 20 millones y 25 millones. En productos de seguros, cuando se vende una gran cantidad, también existen descuentos por volumen. Cuanto mas el cliente compra, mas barato sale el precio por unidad, el mismo concepto se aplica en seguros cibernéticos. Hasta 5 millones, cada millón costaría lo mismo.

Empezando a partir de 10 millones, se aplica un descuento de 5% a cada 5 millones adicionales. Entonces, extrapolar una prima de una capacidad baja para conseguir una prima para una capacidad mas alta requiere la aplicación de un descuento adecuado que esta incluido automáticamente en la herramienta.

En cuanto a las condiciones de mercado, hay 3 posibles selecciones: un mercado neutro, un mercado optimista y un mercado pesimista. La opción bajo condiciones neutras demuestra el precio según el modelo de regresión sin ajustes. La opción bajo condiciones optimistas demuestra el precio considerando un mercado con poco riesgo y mas competencia, resultando en primas mas baratas. La opción bajo condiciones pesimistas demuestra el precio considerando un mercado con mucho riesgo y incertidumbre, resultando en primas mas caras. Como sugerencia, se aplica un aumento/una disminución de prima del 30%, pero estos valores son ajustables según las preferencias necesarias. El deducible aplicable sigue las instrucciones anteriores, por lo tanto, se aplica una cantidad predeterminada dependiendo de la categoría de ganancias en la cual se encuentra la empresa evaluada.

DISCUSIÓN

PONER LA HERRAMIENTA EN PRACTICA

Si calculamos el precio de póliza más bajo posible con la herramienta, en realidad es un poco más alto que la intercepción (precio base). Debido a las restricciones del modelo, es necesario excluir a todas las empresas con menos que 2 mil millones de capitalización de mercado y menos que 6 mil millones de ganancias.

MC						
Market Cap						
2.000.000.000	$ 2.000.000.000,00					
EHL						
Real Revenue	Susceptibility					
6.000.000.000	87%	$ 2.579.051,38				
	87%					
EDBE						
Estimated Record Count	Employee Count	PCI	Probability of Data Breach Incident	Nationality		
		94%	28%	0	$ -	
		94%	*28%*	*0*		
M						
Avg. annual loss (AAL)	Motivation	External Presence (0, 4)	Social Media Presence (0, 4)	Web Popularity (0, 4)	Publicity (0, 4)	
	81%	3	1	3	2	$ -

Fig. 16

Considerando estas limitaciones y suponiendo que nuestra empresa teóricamente no guarda ningún set de datos ni existen perdidas anteriores por incidentes cibernéticos, la calculadora nos da una prima de USD 8.705,60 / millón. Suponiendo que el escenario optimista provoca un descenso de primas de 15% y el escenario pesimista provoca un aumento de primas de 20%, la tabla de primas da lo siguiente:

Primary Premium / Mn	**RoL**	**Payback Period**			
$ 8.705,60	0,87%	115			
Primary Limit (Mn)	5	10	15	20	25
Discount Factor for Streched Layer	100%	95%	90%	85%	80%
Premium (neutral)	$ 43.527,99	$ 82.703,18	$ 117.525,57	$ 147.995,16	$ 174.111,96
Premium (optimistic)	$ 36.998,79	$ 70.297,70	$ 99.896,74	$ 125.795,89	$ 147.995,16
Premium (pesimistic)	$ 52.233,59	$ 99.243,82	$ 141.030,68	$ 177.594,20	$ 208.934,35

Fig. 17

Suponiendo un recuento estimado de datos de 20 millones sets de datos, 10.000 empleados y una pérdida promedia anual de USD 3 millones, la misma empresa debería pagar casi USD 3.000 por millón mas que antes.

Primary Premium / Mn	**RoL**	**Payback Period**			
$ 11.517,21	1,15%	87			
Primary Limit (Mn)	5	10	15	20	25
Discount Factor for Streched Layer	100%	95%	90%	85%	80%
Premium (neutral)	$ 57.586,06	$ 109.413,51	$ 155.482,36	$ 195.792,60	$ 230.344,23
Premium (optimistic)	$ 48.948,15	$ 93.001,48	$ 132.160,00	$ 166.423,71	$ 195.792,60
Premium (pesimistic)	$ 69.103,27	$ 131.296,21	$ 186.578,83	$ 234.951,12	$ 276.413,08

Fig. 18

El impacto es aún más significativo cuando se observan los cambios de primas para capacidades más grandes. Por ejemplo, para 15 millones de seguro bajo condiciones neutras, la prima tiene una diferencia de USD 38.000 entre los dos ejemplos.

INTERPRETACIÓN DE LOS RESULTADOS

Después de poner en práctica la herramienta, los resultados parecen ser muy razonables y aplicables. La certeza sobre la precisión de estos cálculos solo se puede dar utilizando la calculadora para ejemplos reales y compararlos continuamente. Sin embargo, hay una alta posibilidades de recibir indicaciones de primas adecuadas, si se respetan las restricciones y pautas para la evaluación. El 83% de las empresas de la muestra tienen entre 10 y 100 mil millones ganancias, con este porcentaje, la porción también cubre el 80% de todos los países de la cartera. Eso significa, los mejores resultados que se pueden conseguir vienen de instituciones financieras del centro y oeste de Europa, con mas que USD 2 mil millones de capitalización de mercado y entre USD 10 y 100 mil millones de ganancias e información sobre el riesgo de primera mano (directamente del cliente o su corredor).

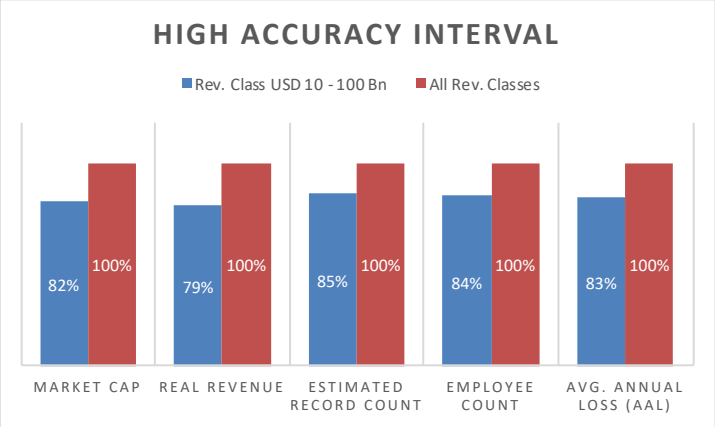


Fig. 19

CONCLUSIÓN

En conclusión, con el fin de contribuir a una posible solución para el problema planteado, se puede considerar cumplido el objetivo principal de este trabajo, que era la creación de una herramienta para dar indicaciones de primas de pólizas cibernéticas. En base a diferentes puntos de vista, limitaciones específicas y factores predeterminados, se pudo crear una herramienta de calificación para las primas de pólizas cibernética de instituciones financieras en Europa, preguntando la cuestión si es posible conseguir un modelo que nos dé resultados confiables. Es evidente, que la definitiva respuesta a esta pregunta solo pueden dar ejemplos reales, pero en la simulación presentada en este trabajo, también se podía demonstrar la funcionalidad y simplicidad de la herramienta. A pesar de la naturaleza de la encuesta y la muestra relativamente limitada, desde una perspectiva teórica se puede decir, que es posible conseguir un modelo que nos dé resultados confiables para dar indicaciones de primas de pólizas cibernéticas. En el caso de que la herramienta resulta ser útil, también se aprueba que se puede estimar una prima de una póliza cibernética con un modelo de regresión lineal. En estudios futuros sobre el tema, se puede considerar experimentar con otros variables o incluso variables adicionales.

REFERENCIAS

1. 2020 Global Insurance Outlook. (2020). Retrieved 30 June 2020, from https://www.ey.com/Publication/vwLUAssets/Insurance_outlook/$FILE/ey-global-insurance-outlook.pdf
2. Cost of a Data Breach Study. (2020). Retrieved 30 June 2020, from https://www.ibm.com/security/data-breach
3. Risk Insights. (2020). Retrieved 30 June 2020, from https://www.guidewire.com/products-new/risk-insights
4. Services, P. (2020). What Is Cybersecurity?. Retrieved 30 June 2020, from https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
5. shish Jain, Vice President & Managing Director, C. (2020). Modelling Cyber Risk. Retrieved 30 June 2020, from https://www.casact.org/community/affiliates/areca/0817/Cyber%20Modeling.pdf
6. Steinberg, J. (2020). Massive Security Breach At Sony -- Here's What You Need To Know. Retrieved 30 June 2020, from https://www.forbes.com/sites/josephsteinberg/2014/12/11/massive-security-breach-at-sony-heres-what-you-need-to-know/#3221145844d8
7. The Global Risks Report 2017. (2020). Retrieved 30 June 2020, from https://www.weforum.org/reports/the-global-risks-report-2017
8. This site produced and maintained Byte Productions, w. (2020). Separating the Truths from the Myths in Cybersecurity. Retrieved 30 June 2020, from https://www.ponemon.org/library/separating-the-truths-from-the-myths-in-cybersecurity
9. Top Five Cyber Risks. (2020). Retrieved 30 June 2020, from https://www.icaew.com/-/media/corporate/files/technical/business-and-financial-management/smes/bas-files/top-five-cyber-risks.ashx?la=en
10. Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies. (2020). Retrieved 30 June 2020, from https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_understanding_cyber_insurance.pdf