نموذج مقترح لقياس أخطار الأمن السيبراني

إعداد

د. جيهان مسعد المعداوي

أستاذ مساعد بقسم الإحصاء التطبيقي والتأمين

كلية التجارة، جامعة المنصورة

gehanelmadawy2020@gmail.com

د. محمد مسعد المعداوي

مدرس بقسم الإحصاء والتأمين

كلية التجارة، جامعة الزقازيق

moh_elmadawye@yahoo.com

د. نها عبد اللطيف عبد الحميد شاهين

أستاذ مساعد بقسم الإحصاء والرياضة والتأمين

كلية التجارة، جامعة كفر الشيخ

Shahinnoha8787@yahoo.com

المجلة العلمية للدراسات والبحوث المالية والتجارية

كلية التجارة – جامعة دمياط

المجلد السادس ــ العدد الأول ــ الجزء الرابع ــ يناير 2025

التوثيق المقترح وفقاً لنظام APA:

المعداوي، جيهان مسعد ؛ **المعداوي**، محمد مسعد ؛ **شاهين**، نها عبد اللطيف عبد الحميد (2025). نموذج مقترح لقياس أخطار الأمن السيبراني، **المجلة العلمية للدراسات والبحوث المالية والتجارية**، كلية التجارة، جامعة دمياط، 6(1)4، 447-471.

رابط المجلة: https://cfdj.journals.ekb.eg/

نموذج مقترح لقياس أخطار الأمن السيبراني

د. جيهان مسعد المعداوي؛ د. محمد مسعد المعداوي؛ د. نها عبد اللطيف عبد الحميد شاهين

ملخص البحث:

يهدف هذا البحث إلى قياس الأخطار السيبرانية (أخطار الهجمات الإلكترونية)، وذلك من خلال نمذجة عدد الأخطار السيبرانية في الأخطار المختلفة عبر مؤسسات مختلفة باستخدام توزيع بواسون وتوزيع ذى الحدين السالب حتى يمكننا التوصل إلى تحديد التوزيع الذى يصف البيانات بشكل أفضل بإيجاد قيمة (log- likelihood)، وقيمة اختبار (Kolmogorov-Smirnov)، وقيمة-P (value)، وأيضًا نمذجة قيم الأخطار السيبرانية فى فئات الأخطار المختلفة وعبر المؤسسات المختلفة باستخدام التوزيع اللوغاريتمى الطبيعى وتوزيع (Skew Normal)، وتم تقدير قيمة كلاً من قيم VaR و TVaR للمؤسسات وللأخطار السيبرانية المختلفة. وكانت أهم النتائج التى توصلت إليها الدراسة، أفضلية استخدام توزيع ذى الحدين السالب عن توزيع بواسون عند توفيق بيانات أعداد الأخطار، وجودة توفيق التوزيع اللوغاريتمى الطبيعى (Log-normal) عن توزيع (Skew-normal. وبتقدير قيمة VaR و TVaR سجلت أخطار "Hack, Fraud, Stolen Computer, Lost Meida" أعلى قيم لكلاً منهما عند مستوى ثقة 99.5%، مما يشير إلى أنها أخطار تشكل تهديدًا ماليًا كبيراً. بينما حققت أخطار Email و Lost Laptop قيم VaR و TVaR منخفضة نسبيًا، مما يشير إلى إنخفاض وطأة الخسارة فى هذه الأخطار. وكانت المؤسسات التجارية هى الأكثر عرضة للخسائر المالية الكبيرة، بينما تواجه المؤسسات الطبية أقل الخسائر. وقد أوصت الدراسة بتوجيه المؤسسات لاستخدام أنظمة الكشف عن الاحتيال والهجمات السيبرانية والوقاية منها. كما توصى بإجراء مزيد من الدراسات الإكتوارية فى التأمين السيبراني (تأمين أخطار الهجمات الإلكترونية) ومحاولة تسعيره.

الكلمات المفتاحية: الأخطار السيبرانية - أخطار الهجمات الإلكترونية - Cyber Risks - Skew-normal distribution - VaR (Value at Risk), TVaR (Tail Value at Risk) .

مقدمة:

تعد الأخطار السيبرانية (مثل الجرائم الإلكترونية، وفشل أو انقطاع تكنولوجيا المعلومات، واختراق البيانات) من بين أكثر الأخطار التجارية أهمية للشركات في جميع أنحاء العالم فى القرن الحادى والعشرين (Allianz Global Corporate & Specialty "AGCS" 2020).

يمكن تعريف الأخطار السيبرانية بأنها "أى خطر ينشأ عن استخدام تكنولوجيا المعلومات والاتصالات (ICT) يعرض سرية البيانات أو الخدمات أو توفرها أو سلامتها للخطر. ويؤدى إضعاف التكنولوجيا التشغيلية (OT) فى النهاية إلى تعطيل الأعمال، وانهيار البنية التحتية، والأضرار المادية التي تلحق بالبشر والممتلكات" (Eling and Schnell 2016a,b). وبشكل عام، يمكن أن تؤدى اختراقات الإلتزامات والسرية المتعلقة بحماية البيانات وانقطاع الأعمال وسرقة البيانات إلى أضرار مالية وخسائر فى السمعة (Cavusoglu *et al.*, 2004; Smith 2004; Salmela 2008; Bulgurcu *et al.*, 2010 and Järveläinen 2013) وبناءًا على ذلك، تعد حلول التأمين مفيدة بشكل خاص لنقل الأخطار من التهديدات الإلكترونية إلى شركات التأمين (Innerhofer-

Oberperfer and Breu 2010; Tosh *et al.*, 2017 and Tonn *et al.*, 2019) ، وكشفت دراسة استطلاعية أجرتها إحدى الشركات العالمية المتخصصة فى الأمن السيبراني "كاسبرسكى" حول "حالة الأمن السيبراني فى القطاع الصناعى 2018"، عن أبرز الدول العربية التى تعرضت لهجمات إلكترونية على شبكاتها وأنظمتها الصناعية، وهى كل من الجزائر بنسبة 66.2% والمغرب بنسبة 60.4% ومصر بنسبة 57.6% والمملكة العربية السعودية بنسبة 48.4% فى مقدمة البلدان التي تواجه مثل تلك الهجمات (الإتحاد المصرى للتأمين، 2019). ولذلك أصبح موضوع الأمن السيبراني من بين أبرز المواضيع التى نالت اهتمام معظم الدول فى الوقت الحاضر وجزءًا أساسيًا من سياستها الوطنية، حيث تصدرت الأخطار السيبرانية مقياس (Allianz) للمخاطر لأول مرة سنة 2020م، وذلك بسبب ازدياد الهجمات الإلكترونية التى تواجه الشركات التجارية (محمد سعيد إسماعيل، 2021). وكاستجابة لهذه الأخطار فإن شركات التأمين تعمل جاهدة على إيجاد طرق لإدارة تلك الأخطار إلا أن سرعة تطور تلك الهجمات وزيادة عددها وتطور المهاجمين وقلة البيانات التاريخية جعل شركات التأمين تواجه عددًا كبيرًا من التحديات نظرًا لصعوبة تقيم الأخطار بدقة، بالإضافة الى عدم قدرة العملاء على تقييم الأخطار التى يوجهوها ويفتقرون إلى الوضوح بشأن خيارات الأمن السيبراني. بالإضافة إلى ذلك، يزداد الأمر سوءًا عند وضع إحتمال تعرض شركات التأمين نفسها لتلك الأخطار وتعرضها للإفلاس، وأيضًا فقد القدرة على إقناع العملاء باتباع سياسة التأمين كأحد أهم طرق إدارة الأخطار. ولذلك تستدعى تلك القضايا إجراء العديد من الأبحاث العلمية التى من شأنها تقديم المساعدة فى إدارة تلك الأخطار التي تهدد الأمن القومى للدولة بالكامل، من خلال تحليل تلك الأخطار والعمل على إيجاد أساليب لمعالجتها (Natalie *et al.*, 2019).

وقد احتل موضوع دراسة الأخطار الإلكترونية (Cyber Risks) الصدارة للبحث عن طرق جديدة تلائم طبيعة تلك الخسائر الفادحة الناتجة عن التعرض للأخطار الإلكترونية، حيث تناولت دراسة (Wendy, 2022) التغلب على عدم الوضوح فيما يتعلق بالتأمين السيبراني كجزء من إستراتيجية إدارة الأخطار بالبنوك، وقد اتبعت هذه الدراسة منهجًا متسلسلًا يتمثل فى إجراء تحليل للمخاطر السيبرانية للبنوك، وأوضح التحليل نقصًا فى المعلومات العلمية لتنفيذ التأمين السيبراني كجزء من إستراتيجية إدارة الأخطار للبنوك. وأوضحت دراسة (Nor *et al.*, 2022) معوقات التأمين السيبراني لكى يمكن التغلب عليها، والعوامل الرئيسية التي تدعم التأمين السيبراني حتى يمكن الاستفادة منها، وذلك لمعرفة أسباب انخفاض الإقبال عليه فى الدول النامية وتحسين الاعتماد على التأمين السيبراني فى هذه الدول. وأما دراسة (Ganbayar *et al.*, 2021) فقد افترضت نهجًا جديدًا لتخفيض تكلفة التأمين السيبراني لمساعدة المؤسسات فى توزيع استثماراتها بطريقة فعالة، وذلك من خلال تخفيض تكلفة التأمين السيبراني بالاعتماد على إتباع طريقة تخفيض الخطر لدى المؤسسات، واختيار ضوابط أمنية أكثر فاعلية، مما يؤدى إلى زيادة الأمان وتقليل تكلفة الحماية التأمينية. وتناولت دراسة (Martin, 2020) قضايا وممارسات التأمين السيبراني، الذى إنتشر بشكل كبير خلال السنوات الأخيرة، والتعريفات التى يمكن الإعتماد عليها للتأمين السيبراني، والطرق القانونية لكتابة العقود، وتأثير ذلك على العقود التأمينية الأخرى، بالإضافة إلى إلقاء الضوء على مشكلة توافر بيانات تاريخية يمكن الاعتماد عليها عند تحليل مخاطر الأمن السيبراني. وأشارت دراسة (Bartlomiej *et al.*, 2019) إلى ضرورة أن تحدد الشركات الناشئة مخاطر تكنولوجيا المعلومات فى مجال نشاطها وتتخذ إجراءات تهدف إلى الحد منها وهو ما يعمل على تحفيز الابتكار في الاقتصاد من المنظور الوطني والدولى. وتناولت دراسة (Damla and Sema 2017) تأثير فائدة التأمين السيبراني على الحماية

الاجتماعية، ونوع المشاكل التي يتعين على شركات التأمين والمؤمن لهم مواجهتها، وتوصلت إلى أنه يمكن تعريف التأمين السيبراني على أنه استثمار أمنى مرتفع عندما يقترن بمستويات متزايدة من الأمان وبنية تحتية قوية لتكنولوجيا المعلومات. وكانت دراسة (Hulisi *et al.*, 2011) من أوائل الدراسات التي تطرقت لمشكلة إدارة أخطار الأمن السيبراني، وهدفت إلى وضع نموذج لإمكانية إثبات الخسائر، وتوصلت إلى أن سياسة التدخل الاجتماعى المناسبة لحث الشركة على الاستثمار فى الحماية الذاتية تعتمد على ما إذا كان بإمكان شركة التأمين التحقق من مستوى الحماية الذاتية، وعند التحقق من مستوى الحماية الذاتية تتمكن شركة التأمين من تصميم عقد مشروط بمستوى الحماية الذاتية، حيث أن التأمين والحماية الذاتية يعتبران مكملين لبعضهما البعض. وتناولت دراسة (Maria *et al.*, 2019) عقود التأمين السيبراني فيما يتعلق بعقود التأمين التقليدية للتأمينات العامة سواء من وجهة نظر المؤمن والمؤمن عليه، وتطرقت إلى بعض المبادئ الاكتوارية الرئيسية فى التسعير وقياس الخطر.

أما دراسة (بانقا، 2019) ركزت على أهمية الأخطار السيبرانية وآثارها الاقتصادية وكيفية إدارتها، والنماذج الدولية التى تأثرت بالهجمات السيبرانية، وحللت أوضاع دول مجلس التعاون الخليجي، وذلك بهدف زيادة الاهتمام بالاستثمار فى الأمن السيبراني ومعرفة الثغرات فى التخطيط الاقتصادى لمجابهة هذه الأخطار، وأوضحت الدراسة أن قطاعات الخدمات المالية والنفط فى قائمة القطاعات المستهدفة عالميًا بالهجمات السيبرانية.

هدفت دراسة (رامز جواد على وآخرون، 2019) إلى توضيح مفهوم جديد في تغطية الأخطار التي تكتتب بها شركات التأمين، كنوع جديد نسبياً للتأمين وهو "التأمين على أخطار الهجمات الإلكترونية" حيث يستخدم هذا النوع من التأمين فى تغطية الأخطار المتعلقة بالبنية التحتية لتكنولوجيا المعلومات وأنشطتها، وتوصلت الدراسة إلى أن الهجمات الإلكترونية من أكبر الأخطار التى تقوم بتغطيتها شركات التأمين وهى متنوعة واحتمال تحققها يتزايد وهذا ما يؤدى إلى فقدان أو سرقة البيانات مما قد يؤدى إلى تحقق الخسائر. كما أوضحت دراسة (محمد سعيد إسماعيل، 2021) أن الشركات التجارية تواجه اليوم تحديات كبيرة فى الحفاظ على سياسة الخصوصية وحماية البيانات وأمن المعلومات. وإدراكًا لهذه التهديدات تدخلت شركات التأمين، وقدمت منتجًا جديدًا نسبيًا، وهو التأمين السيبراني، أو ما يطلق عليه بالتأمين الإلكتروني، ويمثل هذا التأمين استجابة لمطالب الشركات بالدفاع عنها، والتخفيف من الأضرار الناتجة عن الهجمات الإلكترونية لأحداث خرق البيانات وانتهاك الخصوصية. وهدفت إلى دراسة المشكلات القانونية للتأمين الإلكتروني ضد الأخطار السيبرانية، فى الوقت الذى تزداد فيه الهجمات الإلكترونية، وفى المقابل يزيد الطلب على التأمين الإلكتروني. كما عرفت دراسة (عمر أنجوم، 2021) الخطر الإلكتروني أو السيبراني بأنه "خطر مهدد ليس فقط للمعدات والأجهزة المعلوماتية المادية، بل محيط بالمنظومات المعلوماتية ومكوناتها اللامادية، وبالتالى يبقى دائمًا واردًا ومحتملًا وغير متوقع الحدوث، ويمكن أن تترتب عنه أضرار مادية جسيمة يصعب تقدير مدى فداحتها في كثير من الأحيان، مما يستلزم تحمله كأى خطر آخر يهدد الأفراد والمؤسسات"، وتعمل صناعة التأمين على تغطيته، كخطر الحريق أو السرقة أو الضياع. وبناءًا على ذلك، تناولت هذه الدراسة ماهية هذا النوع من الأخطار، ومدى قابلية احتوائها ضمن ما توفره صناعة التأمين من تغطية وضمان، ومعالجة التحديات التى تواجهها هذه الصناعة بالنظر لطبيعة هذا الخطر وخصوصياته، والحلول التى يمكن طرحها لتجاوز هذه التحديات. وتناولت

دراســة (El Bolkiny *et al.*, 2018) إلى دراســة طرق مختلفة من إعادة التأمين وتحديد الحد المناسـب لحد الاحتفاظ فى السـوق المصـرى باسـتخدام Value at risk و Conditional tail expectation لتحليل خصـائص المطالبات الإجمالية واسـتخدام مقياس تعظيم العائد على رأس المال لتحديد حد الاحتفاظ المناسب.

وتتمثل مشـكلة البحث أنه في السـنوات الأخيرة، واجهت الشـركات في جميع أنحاء العالم نوعًا جديدًا من الأخطار، ألا وهو الأخطار السـيبرانية، التى ظهرت كواحدة من أكبر التحديات فى إدارة الأخطار. ولم يتم تطبيق التأمين السـيبراني إلا مؤخرًا، وأصـبح جزءًا متزايدًا من عملية إدارة الأخطار، مما فرض العديد من التحديات على خبراء التأمين، مما دعت الحاجة إلى دراسـة الأخطار السـيبرانية من الناحية التأمينية باسـتخدام المبادئ الاكتوارية الرئيسـية من خلال نمذجة عدد وقيم الأخطار السيبرانية وقياس هذه الأخطار من خلال تقديرالقيمة المعرضـة للخطر وقيمة ذيل الخسـارة المعرضة للخطر.

ويهدف هذا البحث إلى قياس الأخطار السيبرانية (أخطار الهجمات الإلكترونية)، وذلك من خلال نمذجة عدد الأخطار السـيبرانية فى الأخطار المختلفة (Fraud, Hack, Email, Web, Stolen Computer, Stolen Computers, Stolen Documents, Stolen Laptop, Snail Mail, Lost Laptop, Lost Media, Lost Tape, Lost Tapes, Unknown loss "Unkn" and All Risk) لعدة مؤسـسـات مختلفة (Biz, Edu, Gov, Med) باسـتخدام توزيع بواسـون وتوزيع ذى الحدين السالب حتى يمكننا التوصل إلى تحديد التوزيع الذى يصف البيانات بشكل أفضل بإيجاد قيمة (log-likelihood)، وقيمة اختبار (Kolmogorov-Smirnov)، وقيمة (P-value)، وأيضًـا نمذجة قيم الأخطار السـيبرانية فى فئات مختلفة للأخطار وعبر مؤسـسـات مختلفة باسـتخدام التوزيع اللوغـاريتمى الطبيعى وتوزيع (Skew-Normal)، ثم تقـدير القيمـة المعرضـــة للخطر (Value at risk "VaR") وتقدير قيمة ذيل الخسـارة المعرضـة للخطر (Tail Value at Risk "TVaR") للمؤسسات وللأخطارالسيبرانية عند مستويات الثقة المختلفة.

وترجع أهمية البحث إلى أن موضـوع الأمن السيبراني أصـبح من أبرز الموضـوعات التى نالت اهتمام معظم الدول فى الوقت الحاضر، حيث صنف المنتدى الاقتصـادى عام 2020م الهجمات الالكترونيـة على أنهـا واحدة من أكبر التهديدات طويلـة المدى التي تواجـه العـالم وذلك فى التقرير السـنوى لتحليل الأخطار (بدر، 2021)، كما تصـدرت الأخطار الإلكترونية السـيبرانية مقياس (Allianz) للمخاطر لأول مرة سـنة 2020م وذلك بسـبب ازدياد مخاطر الهجمات الإلكترونية التى أصـبحت جزءًا من الخطط الحديثة للحروب بين المؤسـسـات. ولذلك فان كافة المؤسـسـات المالية والحكومية تقابل فى الوقت الحالى تحديات كبيرة فى مواجهة الأخطار السـيبرانية، وذلك لحداثة هذا النوع من الأخطار ومن هنا تأتى أهمية هذا البحث لعدة أسباب أهمها:

- تطور الهجمات الالكترونية بشكل سريع ومستمر.
- قلة البيانات التاريخية المتاحة نظرًا لحداثة مخاطر الهجمات الإلكترونية.
- ارتفاع الخسائر الناتجة عن الهجمات الإلكترونية وعدم القدرة على إثبات تلك الخسائر.
- تعرض المؤسسات الحكومية والمالية لمخاطر الهجمات الإلكترونية بعد التحول الرقمى.
- تعدد أنواع الأخطار المترتبة على الهجمات الإلكترونية حيث قد تخسر بعض المؤسسات سمعتها نتيجة لتلك الهجمات.

- عدم فاعلية دور التأمين على تلك الخسائر المترتبة على هذه الهجمات إن لم يكن هناك العديد من وسائل إدارة الأخطار بالمؤسسة أو المنظمة قبل اللجوء لنظام التأمين.

الدراسة التطبيقية:

نظرًا لعدم توافر بيانات عن الأخطار السيبرانية فى جمهورية مصر العربية. لذا، ستعتمد الدراسة التطبيقية فى هذا البحث على بيانات الأخطار الخاصة بالأمن السيبراني والمتاحة على الموقع الإلكتروني التالي: (http://attrition.org/dataloss/dldos.html)

وقد تم الحصول على أعداد المشاهدات وفقًا لنوع المؤسسات ونوع الأخطار السيبرانية (الإلكترونية)، حيث كان عدد المشاهدات الإجمالي 765 موزعة وفقًا لنوع المؤسسة ونوع الأخطار السيبرانية على النحو الموضح في جدول (1).

جدول (1): يوضح عدد المشاهدات لأنواع الأخطار السيبرانية لعدة مؤسسات مختلفة:

نوع الأخطار الإلكترونية	نوع المؤسسة				
	Biz	**Edu**	**Gov**	**Med**	**All**
Fraud	29	3	11	8	51
Hack	56	102	23	3	184
Email	2	9	6	1	18
Web	24	61	32	13	130
Stolen Computer	13	13	10	15	51
Stolen Computers	5	5	7	4	21
Stolen Documents	6	5	7	1	19
Stolen Laptop	59	40	44	35	178
Snail Mail	8	6	16	3	33
Lost Laptop	1	0	2	2	5
Lost Media	8	5	15	6	34
Lost Tape	6	0	6	0	12
Lost Tapes	11	0	1	1	13
Unknown Loss (unkn)	5	5	6	0	16
All Risk (Data)	233	254	186	92	765

حيث أن: Biz: ترمز للمؤسسة التجارية ، Edu: ترمز للمؤسسة التعليمية، Gov: ترمز للمؤسسة الحكومية، Med: ترمز للمؤسسة الطبية.

تم استخدام برنامج (R) فى توفيق بيانات أعداد وقيم الأخطار السيبرانية وتقدير قيمة VaR و TVaR للمؤسسات وللأخطار السيبرانية المختلفة (Goulet, 2007; R Development Core Team, 2007 and Delignette-Muller and Dutang, 2015) .

أولاً: توفيق بيانات أعداد الأخطار السيبرانية:

تم استخدام توزيع بواسون وتوزيع ذى الحدين السالب حيث انهما أكثر التوزيعات شيوعاً في الأدبيات الاكتوارية لتوفيق بيانات أعداد الأخطار.

(1) توفيق بيانات أعداد الأخطار السيبرانية وفقاً لتوزيع بواسون:

وتكون دالة الكتلة الاحتمالية (Probability Mass Function (PMF)) لتوزيع بواسون (Aman Agrawal, 2024 and Marco Taboga, 2021) على الصورة التالية:

$$\mathbf{P(Z=z)} = \frac{\lambda^z e^{-\lambda}}{z!} \quad , \quad \mathbf{z=0,1,2,\ldots} \quad , \quad \boldsymbol{\lambda > 0}$$

$\mathbf{Z}$: تمثل عدد الأخطار السيبرانية ، $\boldsymbol{\lambda}$: متوسط عدد الأخطار السيبرانية

$$E(Z) = Var(Z) = \lambda$$

يكثر استخدام توزيع بواسون فى الحالات التى تقع فيها الأحداث وفقا لمعدلات زمنية، وكذلك فى حالة الأحداث نادرة الوقوع.

وتكون دالة الإمكان الأعظم لتوزيع بواسون لعدد من المشاهدات ($z_1, z_2, z_3, \ldots\ldots\ldots, z_n$) على النحو التالى:

$$\boldsymbol{L(\lambda; z_1, z_2, z_3, \ldots\ldots\ldots, z_n) = \prod_{j=1}^{n} \frac{\lambda^{z_j} e^{-\lambda}}{z_j!}}$$

وللحصول على اللوغاريتم الطبيعى لدالة الإمكان الأعظم (the natural log-likelihood function) لتوزيع بواسون يكون على النحو التالى:

$$\boldsymbol{\ln L(\lambda; z_1, z_2, z_3, \ldots\ldots\ldots, z_n) = \ln\left(\prod_{j=1}^{n} \frac{\lambda^{z_j} e^{-\lambda}}{z_j!}\right)}$$

$$\boldsymbol{\ln L(\lambda; z_1, z_2, z_3, \ldots\ldots\ldots, z_n) = \sum_{j=1}^{n} \ln\left(\frac{\lambda^{z_j} e^{-\lambda}}{z_j!}\right)}$$

$$\boldsymbol{\ln L(\lambda; z_1, z_2, z_3, \ldots\ldots\ldots, z_n) = \sum_{j=1}^{n} \left[\ln(\lambda^{z_j}) + \ln(e^{-\lambda}) - \ln(z_j!)\right]}$$

$$\boldsymbol{\ln L(\lambda; z_1, z_2, z_3, \ldots\ldots\ldots, z_n) = \sum_{j=1}^{n} \left[z_j \ln(\lambda) - \lambda - \ln(z_j!)\right]}$$

فى حالة إيجاد المضـــروب لقيمة عددية كبيرة يتم إســتخدام (Stirling's approximation) وهى كالتالى:

$$\ln z! = z \ln z - z$$

(2) توفيق بيانات أعداد الأخطار السيبرانية وفقاً لتوزيع ذى الحدين السالب:

توزيع ذى الحدين السالب هو توزيع احتمالى منفصل يستخدم غالبًا لنمذجة بيانات الأعداد، يتم تطبيقه عمومًا عندما يكون تباين البيانات أكبر من المتوسط (التشتت الزائد). على النقيض من ذلك، يفترض توزيع بواسون أن المتوسط والتباين متساويان، وهو ما لا يحدث دائمًا فى البيانات الواقعية.

وتكون دالـة الكتلـة الاحتمـاليـة (Probability Mass Function 'PMF') لتوزيع ذى الحـدين السالب (Jakub *et al.*, 2022) على الصورة التالية:

$$\boldsymbol{P(Z = k) = \binom{k + r - 1}{k} p^r (1 - p)^k , \qquad k = 0, 1, 2, ...}$$

k: تمثل عدد الأخطار السيبرانية ، $\boldsymbol{r}$: عدد محاولات النجاح ، p : احتمال النجاح (احتمال وقوع الخطر)

$$E(Z) = \frac{r(1-p)}{p}, \qquad Var(\boldsymbol{Z}) = \frac{r(1-p)}{p^2}$$

وللحصـــول على اللوغاريتم الطبيعى لدالة الإمكان الأعظم (log-likelihood function) لتوزيع ذى الحدين السالب يكون على النحو التالى:

$$\boldsymbol{\ln L(r, p) = \sum_{j=1}^{n} \left[\ln \binom{k_j + r - 1}{k_j} + r \ln p + k_j \ln(1 - p) \right]}$$

k_j: تمثل عدد الأخطار السيبرانية

$$\boldsymbol{\binom{k_j + r - 1}{k_j} = \frac{(k_j + r - 1)!}{(k_j!)(r - 1!)} = \frac{\Gamma(k_j + r)}{\Gamma(k_j + 1) * \Gamma(r)}}$$

وتم تطبيق توزيع بواســون، وتوزيع ذى الحدين الســالب على كل من البيانات الكاملة وعلى كلاً من المؤسـســة التجارية (Biz) والمؤسـســة التعليمية (Edu) فى الأنواع المختلفة للأخطار وعلى عدد الأخطار السيبرانية لأخطار (Hack, Stolen Laptop) فى المؤسسات المختلفة حيث أنهم يحققون أعلى عـدد للحوادث الســيبرانيـة. وتم اختبـار جودة التوفيق للتوزيع من خلال إيجـاد قيمـة (log-likelihood) ، وقيمة اختبار (Kolmogorov-Smirnov)، وقيمة (P-value) كما هو موضـــح في جدول (2).

جدول (2): يوضح قيمة (log-likelihood)، وقيمة اختبار (Kolmogorov-Smirnov)، وقيمة (P-value) لأعداد الأخطار السيبرانية لمجموعة البيانات الكاملة وبعض المجموعات الفرعية.

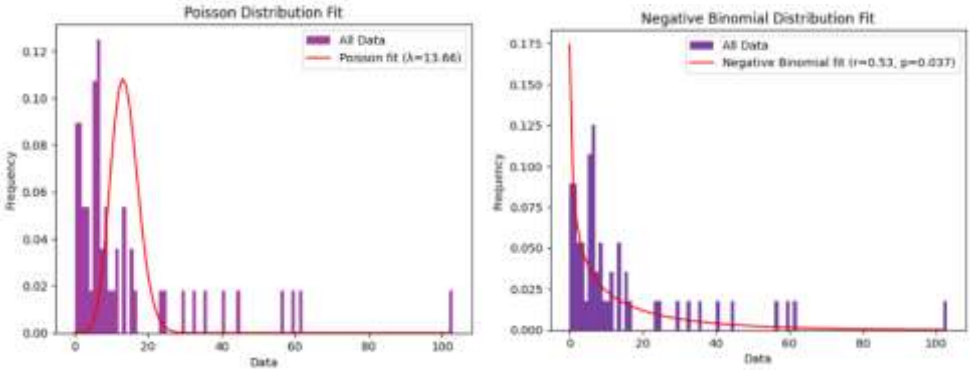
Model	Data	Log-likelihood	KS	P-value
Poisson	All Data	-625.79	0.552	1.49×10^{-16}
Negative Binomial	All Data	-203.89	0.174	0.059*
Poisson	Biz	-145.43	0.556	0.00013
Negative Binomial	Biz	-53.91	0.181	0.681*
Poisson	Edu	-256.75	0.70	2.11×10^{-7}
Negative Binomial	Edu	-51.87	0.210	0.503*
Poisson	Hack	-78.26	0.50	0.188
Negative Binomial	Hack	-19.62	0.218	0.971*
Poisson	Stolen Laptop	-14.71	0.240	0.933*
Negative Binomial	Stolen Laptop	-14.31	0.231	0.952*

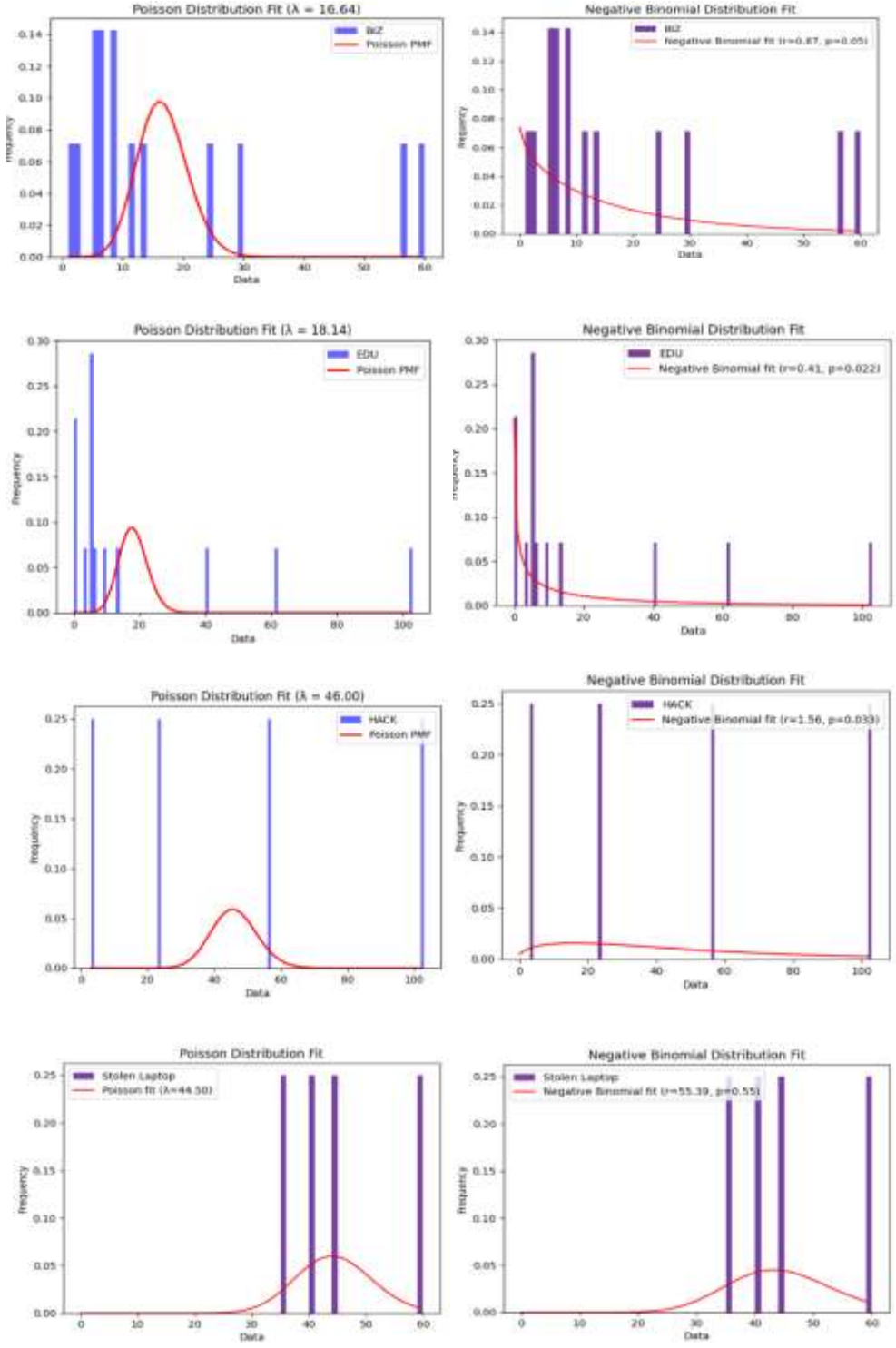
* تم إيجاد قيمة log-likelihood , Kolmogorov-Smirnov (KS), p-value باستخدام برنامج R.

* التوزيع يناسب البيانات.

بشكل عام، بالنسبة لعدد الأخطار السيبرانية، كانت نتائج توزيع بواسون غير ملائمة من حيث جودة التوفيق بالنسبة لمجموعة البيانات الكاملة (All Data)، وأيضا للمجموعات الفرعية (Biz, Edu, Hack) بسبب التشتت الزائد في البيانات، ماعدا عدد أخطار (Stolen Laptop) فأعطت نتائج جيدة من حيث جودة التوفيق لتوزيع بواسون، وللتغلب على مشكلة التشتت الزائد في البيانات، تم استخدام توزيع ذى الحدين السالب لتوفيق البيانات، فكانت نتائجها جيدة ($p>0.05$) من حيث جودة التوفيق فى (All Data, Biz, Edu ,Hack, Stolen Laptop).

والأشكال التالية توضح توفيق (All data, Biz, Edu, Hack, Stolen Laptop) بالنسبة لتوزيع بواسون، وتوزيع ذى الحدين السالب باستخدام برنامج R:




Poisson Distribution Fit (λ = 16.64)
BIZ
Poisson PMF
Negative Binomial Distribution Fit
BIZ
Poisson Distribution Fit (λ = 18.14)
EDU
Poisson PMF
Negative Binomial Distribution Fit
EDU
Negative Binomial fit (r=0.41, p=0.022)
Poisson Distribution Fit (λ = 46.00)
HACK
Poisson PMF
Negative Binomial Distribution Fit
HACK
Negative Binomial fit (r=1.56, p=0.033)
Poisson Distribution Fit
Stolen Laptop
Poisson fit (λ=44.50)
Negative Binomial Distribution Fit
Stolen Laptop
Negative Binomial fit (r=55.39, p=0.55)
Frequency
Data

ثانياً: توفيق بيانات قيم الأخطار السيبرانية:

(1) توفيق بيانات قيم الأخطار السيبرانية وفقاً للتوزيع اللوغاريتمى الطبيعى (log-normal):

وتكون دالـة الكثـافـة الاحتمـاليـة (Probability Density Function (PDF)) للتوزيع اللوغـاريتمى الطبيعى (William L. Dunn, J. Kenneth Shultis, 2023) على الصـــورة التالية:

$$f(x;\ \mu,\sigma^2) = \frac{exp\left\{-\frac{1}{2}\left(\frac{\ln x-\mu}{\sigma}\right)^2\right\}}{x\sigma\sqrt{2\pi}}$$

$$-\infty < \mu < \infty\ ,\qquad \sigma > 0\ \ ,x > 0$$

$$E(X) = e^{\mu+\frac{1}{2}\sigma^2}$$

$$Var(X) = \left(e^{2\mu+\sigma^2}\right) \times (e^{\sigma^2} - 1)$$

وللحصـول على اللوغاريتم الطبيعى لدالة الإمكان الأعظم (log- likelihood function) للتوزيع اللوغاريتمى الطبيعى يكون على النحو التالى:

$$L(\mu,\sigma^2) = \prod_{j=1}^{n} f(x_j;\ \mu,\sigma^2)$$

$$\ln L(\mu,\sigma^2) = \sum_{j=1}^{n}\left[\ln\left(\frac{exp\left\{-\frac{1}{2}\left(\frac{\ln x_j-\mu}{\sigma}\right)^2\right\}}{x_j\sigma\sqrt{2\pi}}\right)\right]$$

$$\ln L(\mu,\sigma^2) = \sum_{j=1}^{n}\left[-\ln(x_j) - \ln(\sigma) - \ln\left(\sqrt{2\pi}\right) - \frac{1}{2}\left(\frac{\ln x_j-\mu}{\sigma}\right)^2\right]$$

$$\ln L(\mu,\sigma^2) = -n\ln(\sigma) - n\ln\left(\sqrt{2\pi}\right) - \sum_{j=1}^{n}\ln(x_j) - \frac{1}{2\sigma^2}\left(\sum_{j=1}^{n}\ln(x_j) - \mu\right)^2$$

(2) توفيق بيانات قيم الأخطار السيبرانية وفقاً لتوزيع skew-normal:

وتكون دالـة الكثـافـة الاحتمـاليـة (Probability Density Function (PDF)) لتوزيع (skew-normal) (Fernanda and Gomes 2011; Grace Ngunkeng, 2013) على الصورة التالية:

$$f(x;\xi,\omega,\alpha) = \frac{2}{\omega}\phi\left(\frac{x-\xi}{\omega}\right)\Phi\left(\alpha\frac{x-\xi}{\omega}\right)$$

$\phi(z)$: دالة كثافة الاحتمال للتوزيع الطبيعى المعيارى وتكون كالتالى:

$$\phi(z) = \frac{1}{\sqrt{2\pi}}e^{\left(-\frac{z^2}{2}\right)}$$

$\Phi(z)$: تمثل دالة التوزيع التراكمية للتوزيع الطبيعى المعيارى.

ξ :location parameter (متوسط التوزيع)، ω :scale parameter (الانحراف المعيارى للتوزيع)، α : shape parameter

$$E(X) = \xi + \omega\delta\sqrt{\frac{2}{\pi}},\ \delta = \frac{\alpha}{\sqrt{1+\alpha^2}}$$

$$\mathrm{Var(X)} = \omega^2(1-\frac{2\delta^2}{\pi})$$

وللحصـــول على اللوغاريتم الطبيعى لدالة الإمكان الأعظم (log-likelihood function) لتوزيع (skew-normal) يكون على النحو التالى:

$$L(\xi,\omega,\alpha) = \prod_{j=1}^{n} f(x_j;\ \xi,\omega,\alpha)$$

$$\ln L(\xi,\omega,\alpha) = \sum_{j=1}^{n} \ln f(x_j;\ \xi,\omega,\alpha)$$

$$\ln L(\xi,\omega,\alpha) = \sum_{j=1}^{n}\left[\ln\left(\frac{2}{\omega}\phi\left(\frac{x_j-\xi}{\omega}\right)\Phi\left(\alpha\frac{x_j-\xi}{\omega}\right)\right)\right]$$

$$\ln L(\xi,\omega,\alpha) = \sum_{j=1}^{n}\left[\ln 2 - \ln\omega + \ln\phi\left(\frac{x_j-\xi}{\omega}\right) + \ln\Phi\left(\alpha\frac{x_j-\xi}{\omega}\right)\right]$$

$$\ln L(\xi,\omega,\alpha) = \left[n\ln 2 - n\ln\omega + \sum_{j=1}^{n}\ln\phi\left(\frac{x_j-\xi}{\omega}\right) + \sum_{j=1}^{n}\ln\Phi\left(\alpha\frac{x_j-\xi}{\omega}\right)\right]$$

جدول (3): يوضح قيمة (log-likelihood)، وقيمة اختبار (Kolmogorov-Smirnov)، وقيمة (P-value) لقيم الأخطار السيبرانية لمجموعة البيانات الكاملة وبعض المجموعات الفرعية.

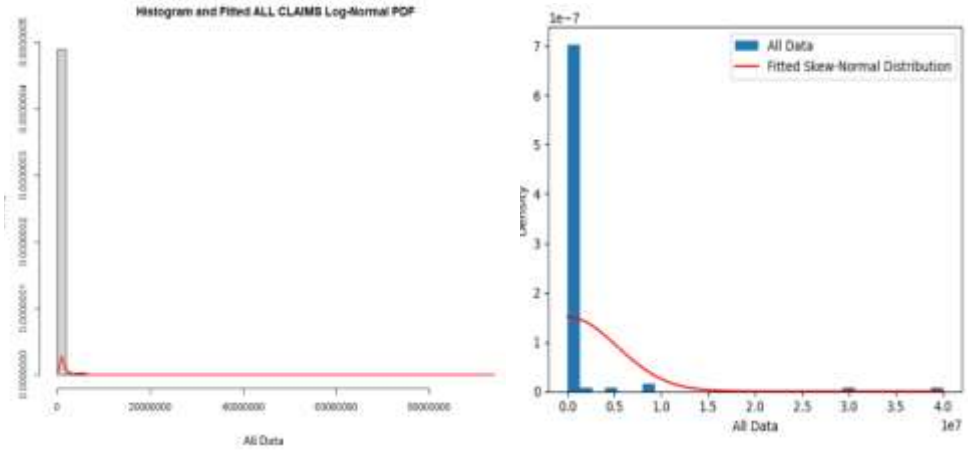
Model	Data	Log-likelihood	KS	P-value
Log-normal	All Data	-8657.5	0.0402	0.1692*
Skew-normal	All Data	-1555.7	0.8594	4.52×10^{-82}
Log-normal	Biz	−2794.9	0.0307	0.976*
Skew-normal	Biz	-1246.3	0.8354	2.38e-57
Log-normal	Edu	-2664.2	0.0439	0.713*
Skew-normal	Edu	-2632.8	0.5130	2.87×10^{-54}
Log-normal	Hack	-2190.8	0.0676	0.372*
Skew-normal	Hack	-2645.5	0.9004	1.03×10^{-159}
Log-normal	Stolen Laptop	-1946.9	0.0430	0.8985*
Skew-normal	Stolen Laptop	-1216.8	0.5820	4.72×10^{-32}

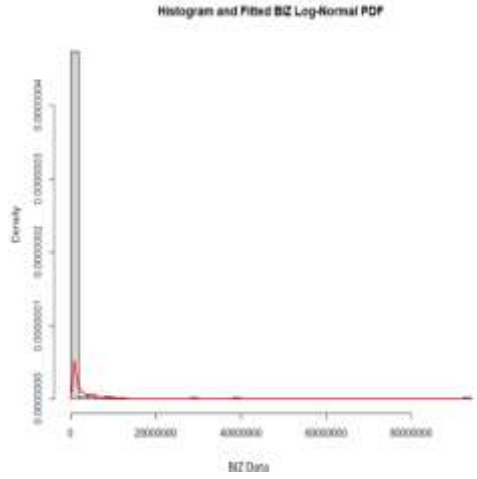
* تم إيجاد قيمة log-likelihood , Kolmogorov-Smirnov (KS), p-value باستخدام برنامج R .

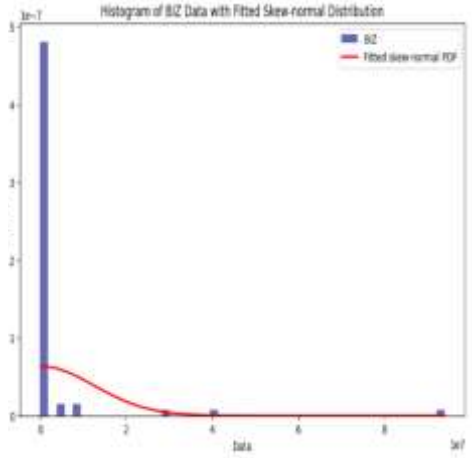
* التوزيع يناسب البيانات.

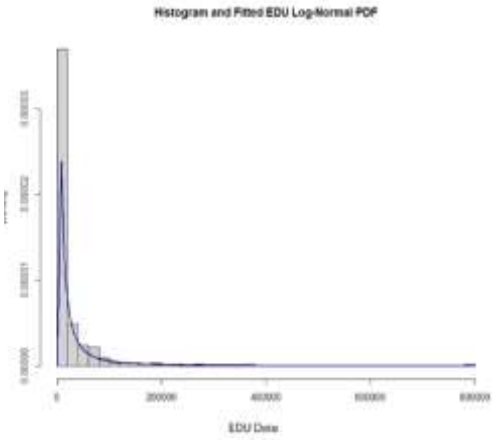
بشكل عام، بالنسبة لقيم الأخطار السيبرانية، فكانت نتائج التوزيع اللوغاريتمى الطبيعى جيدة من حيث جودة التوفيق بالنسبة لمجموعة البيانات الكاملة وللمجموعات الفرعية (All Data, Biz, Edu ,Hack, Stolen Laptop) حيث كانت قيمة ($p>0.05$)، أما نتائج توزيع (Skew- normal) فكانت غير ملائمة من حيث جودة التوفيق بالنسبة لمجموعة البيانات الكاملة وللمجموعات الفرعية.

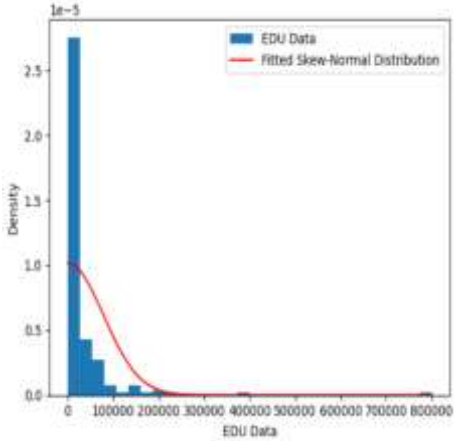
والأشكال التالية توضح توفيق (All data, Biz, Edu, Hack, Stolen Laptop) بالنسبة لتوزيع (Log -normal) وتوزيع (Skew- normal) باستخدام برنامج R:

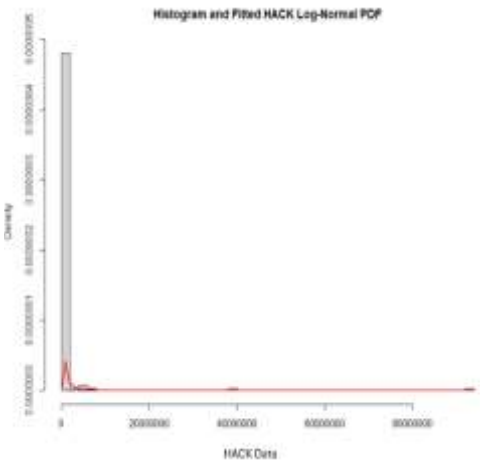


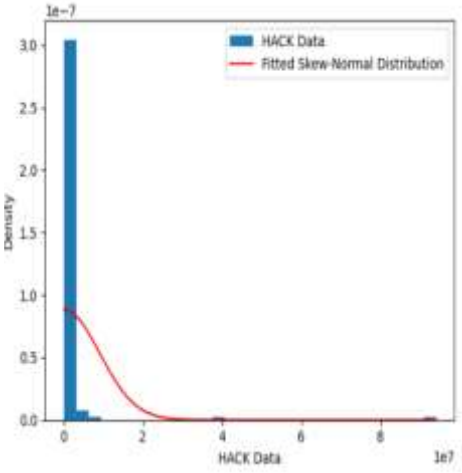

Histogram and Fitted BIZ Log-Normal PDF
Density
BIZ Data

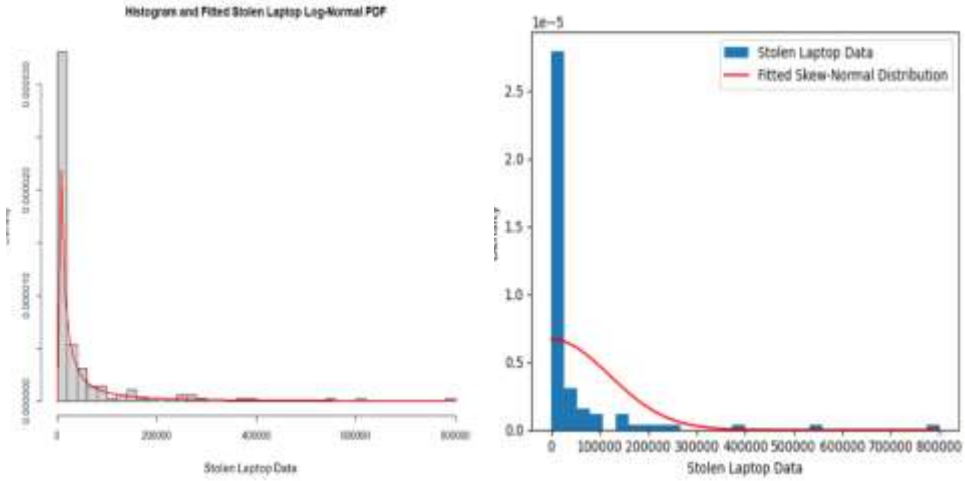

Histogram of BIZ Data with Fitted Skew-normal Distribution
BIZ
Fitted skew-normal PDF
1e-7
Data


Histogram and Fitted EDU Log-Normal PDF
EDU Data


1e−5
EDU Data
Fitted Skew-Normal Distribution
Density
0 100000 200000 300000 400000 500000 600000 700000 800000
EDU Data


Histogram and Fitted HACK Log-Normal PDF
Density
HACK Data


1e−7
HACK Data
Fitted Skew-Normal Distribution
Density
HACK Data
1e7



ثالثاً: قياس الخطر:

1) القيمة المعرضة للخطر Value at Risk (VaR) :

هى مقياس يستخدم لتقييم الخسارة المحتملة فى قيمة المحفظة خلال فترة زمنية محددة لفترة ثقة معينة. وتعرف القيمة المعرضة للخطر عند مستوى الثقة α للمتغير العشوائي X بـ $\mathrm{VaR}_\alpha(X)$ (Andreas 2000; Abraham 2010; Stuart A. Klugman *et al.*, 2019, and El Bolkiny *et al.*, 2018) كالتالى:

$$\mathrm{VaR}_\alpha(X) = F_X^{-1}(\alpha)$$

$\mathrm{VaR}_\alpha(X)$: تشير إلى القيمة المعرضة للخطر عند مستوى الثقة α لمتغير عشوائى X

$F_X^{-1}(\alpha)$: (inverse Cumulative Distribution Function) أو (quantile function) وهى تمثل العملية العكسية لدالة التوزيع التراكمية أى أنها قيمة x التي تجعل "$P(X \leq x) = \alpha$".

2) قيمة ذيل الخسارة المعرضة للخطر Tail Value at Risk (TVaR):

هو مقياس يستخدم لتقييم متوسط الخسائر فى حال تجاوز الخسائر قيمة **VaR** عند المستوى α للتوقع الشرطى (Denuit *et al.*, 2005 ; Hardy 2006 and El Bolkiny *et al.*, 2018) ، ويمكن عرضها على النحو التالى:

$$\mathrm{TVaR}_\alpha(X) = \mathrm{E}[X \mid X > \mathrm{VaR}_\alpha(X)]$$

α : مستوى الثقة (على سبيل المثال، 95% أو 99%).

VaRα : قيمة الـ VaR عند مستوى الثقة α

X : المتغير العشوائى الذى يمثل قيمة الخسارة.

$\mathrm{E}[X \mid X > \mathrm{VaR}_\alpha]$: القيمة المتوقعة (المتوسط) للخسائر بشرط أن تكون الخسائر أكبر من VaRα.

ويمكن حساب TVaR باستخدام الصيغة التالية:

$$\mathrm{TVaR}_{\alpha} = \mathrm{E}[X \mid X > \mathrm{VaR}_{\alpha}] = \frac{1}{1-\alpha}\int_{\mathrm{VaR}_{\alpha}}^{\infty} x f_X(x)\, dx$$

وسوف يتم إيجاد القيمة المعرضة للخطر (VaR) وقيمة ذيل الخسارة المعرضة للخطر (TVaR) باستخدام برنامج R للمؤسسات والأخطار السيبرانية المختلفة وفقًا لمستويات الثقة المختلفة (99.5%، 99%، 97.5%، 97%، 95%، و90%)، كما هو موضح في جدول (4 و 5)، حيث تبين ما يلي:

- سجلت أخطار "Hack, Fraud, Stolen Computer, Lost Meida" أعلي قيم لكلاً من VaR و TVaR مقارنة ببقية الأخطار الأخري عند مستوى ثقة 99.5%، مما يشير إلى أنها أخطار تشكل تهديدًا ماليًا كبيراً.
- حققت أخطار Email و Lost Laptop قيم VaR و TVaR منخفضة نسبيًا، مما يشير إلى إنخفاض وطأة الخسارة فى هذه الأخطار.
- كانت المؤسسات التجارية هى الأكثر عرضة للخسائر المالية الكبيرة، بينما حققت المؤسسات الطبية أقل الخسائر.
- كانت قيم TVaR دائمًا أعلى من قيم VaR لنفس الخطر وكذلك مستوى الثقة، مما يعكس قيمة الخسارة المتوقعة فى أسوأ حالات الخسارة والتي تتخطي قيمة VaR.
- ثبات قيمة TVaR عند مستوى ثقة معين واستمرار ثباتها عند مستويات الثقة التالية الأعلى، يشير إلى أن قيم الخسائر الكبيرة فى ذيل التوزيع أصبحت مستقرة نسبيا عند هذا المستوى وكذلك المستويات الأعلى.

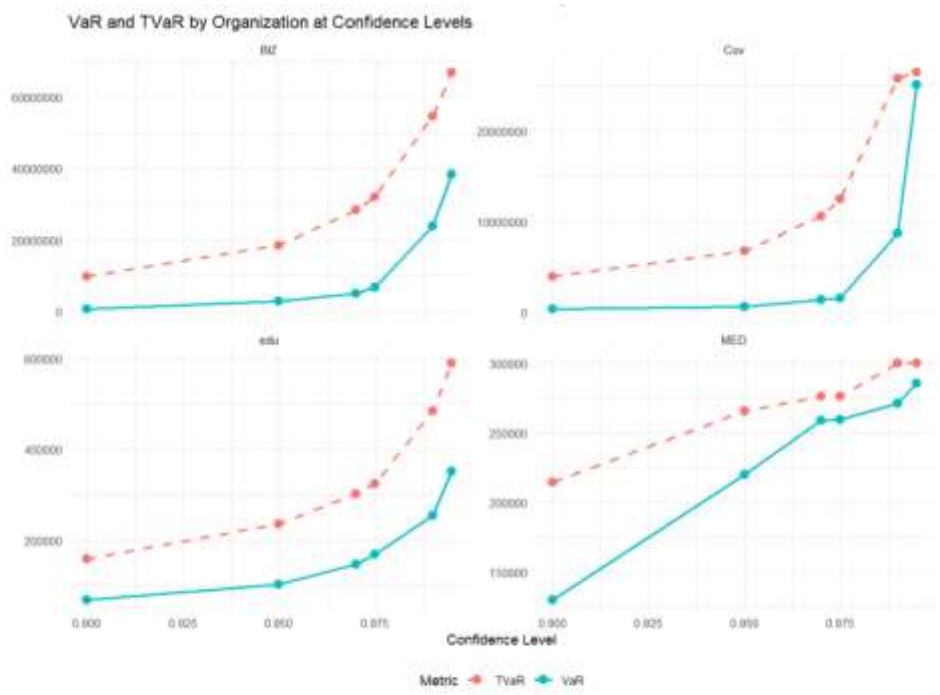
جدول (4): يوضح Value at Risk (VaR) و Tail Value at Risk (TVaR) بالنسبة للمؤسسات عند مستويات الثقة المختلفة.

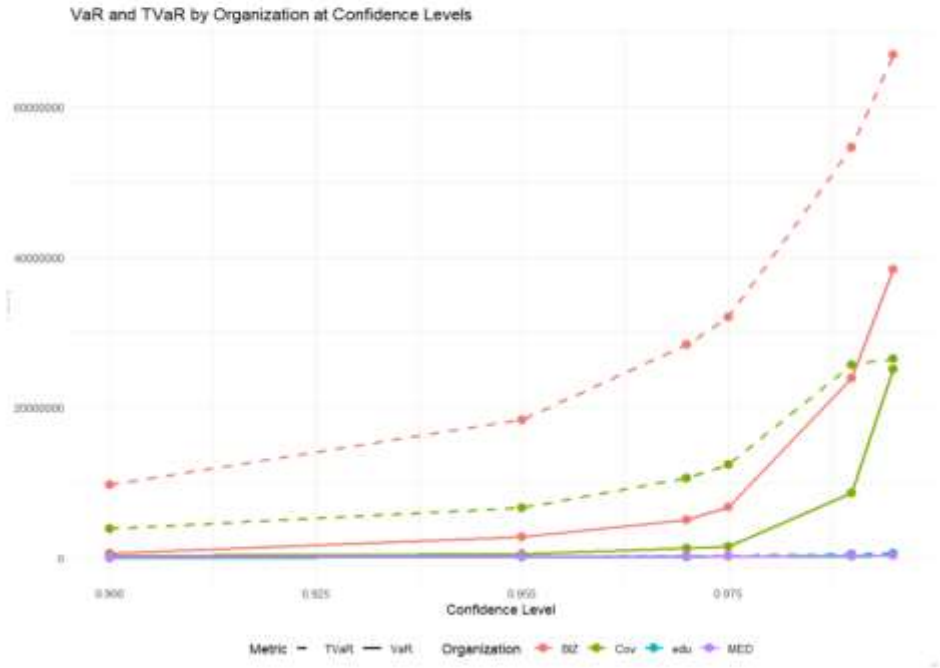
المؤسسة	Risk Measure	(VaR) and (TVaR)					
		90%	95%	97%	97.5%	99%	99.5%
Biz	VaR	628736	2760000	5052000	6740000	23920000	38400000
	TVaR	9714326	18336450	2848201	32022901	54666667	67000000
Edu	VaR	68500	102100	147050	168900	254100	350850
	TVaR	158105	235040	301565	233217	48333	590000
Gov	VaR	300000	559300	1342000	1540000	8660000	25105000
	TVaR	3911432	6684777	10600000	12440000	25750000	26500000
Med	VaR	129800	220000	258394	259395	270880	285440
	TVaR	214180	265560	276000	276000	300000	300000

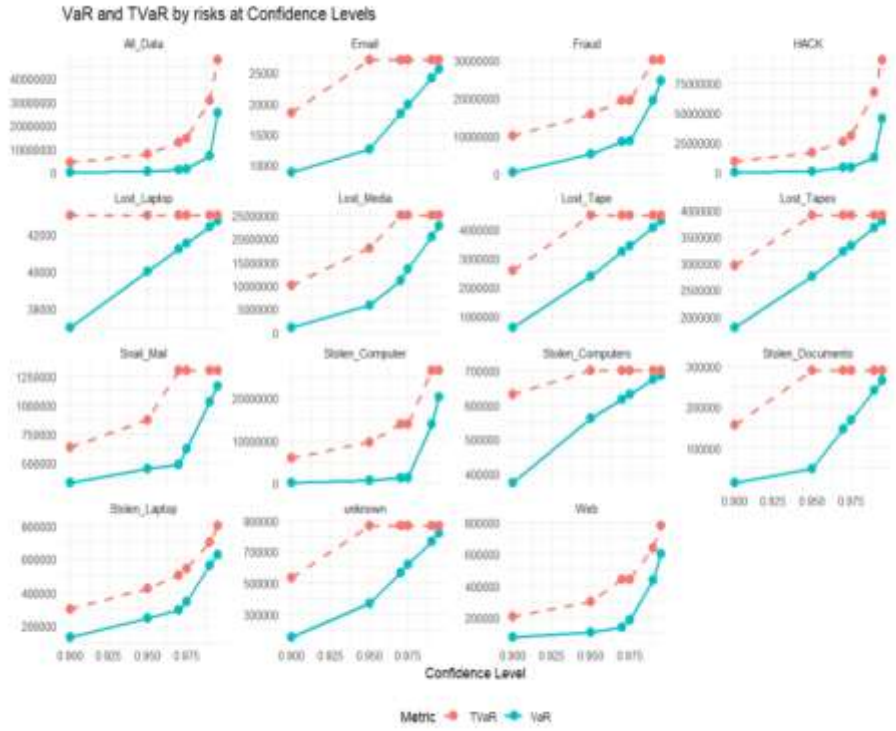
جدول (5): يوضح Value at Risk (VaR) و Tail Value at Risk (TVaR) بالنسبة للأخطار السيبرانية عند مستويات الثقة المختلفة.

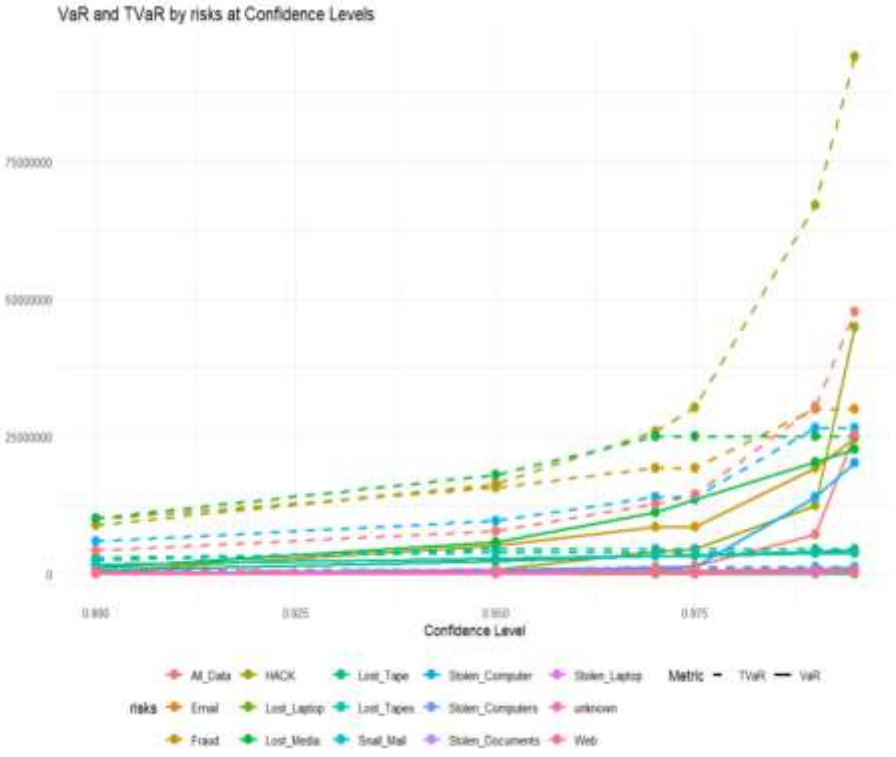
الأخطار السيبرانية	Risk Measure	(VaR) and (TVaR)					
		90%	95%	97%	97.5%	99%	99.5%
Fraud	VaR	465000	5150000	8568703	8603054	19318703	24659351
	TVaR	9922681	15712468	19318703	19318703	30000000	30000000
Hack	VaR	237200	784842	4108000	4560000	12366000	44860000
	TVaR	8793127	16379600	25916667	30260000	67000000	94000000
Email	VaR	8880	12550	18330	19775	24110	25555
	TVaR	18500	27000	27000	27000	27000	27000
web	VaR	71400	104650	137620	185350	433300	599400
	TVaR	203219	299143	438000	438000	640000	780000
Stolen Computer	VaR	160000	754500	1184500	1292250	13950000	20225000
	TVaR	5919200	9623000	13950000	13950000	26500000	26500000
Stolen Documents	VaR	14600	47900	144740	168950	241580	265790
	TVaR	155500	290000	290000	290000	290000	290000
Snail Mail	VaR	332000	447000	484000	620000	1028000	1164000
	TVaR	636250	875000	1300000	1300000	1300000	1300000
Lost Laptop	VaR	37000	40000	41200	41500	42400	42700
	TVaR	43000	43000	43000	43000	43000	43000
Lost Media	VaR	1051000	5735000	11140000	13450000	20380000	22690000
	TVaR	10050000	18000000	25000000	25000000	25000000	25000000
Lost Tape	VaR	605000	2382500	3229500	3441250	4076500	4288250
	TVaR	2575000	4500000	4500000	4500000	4500000	4500000
Lost Tapes	VaR	1800000	2760000	3216000	3330000	3672000	3786000
	TVaR	2950000	3900000	3900000	3900000	3900000	3900000
Stolen Computers	VaR	375000	562000	617200	631000	672400	686200
	TVaR	631000	700000	700000	700000	700000	700000
Stolen Laptop	VaR	130900	245220	293800	346000	562826	628104
	TVaR	299920	424840	502961	543553	702883	800000
Unknown (unkn)	VaR	150000	366750	566850	616875	766950	816975
	TVaR	533500	867000	867000	867000	867000	867000
All Data (Risk)	VaR	200000	497000	1042000	1491200	7136000	25285000
	TVaR	4233759	7767554	12684061	14386670	30454676	47625000

والأشكال التالية توضح (VaR) و (TVaR) بالنسبة للمؤسسات وللأخطار السيبرانية عند مستويات الثقة المختلفة باستخدام برنامج R:






VaR and TVaR by risks at Confidence Levels
All_Data
Email
Fraud
HACK
Lost_Laptop
Lost_Media
Lost_Tape
Lost_Tapes
Snail_Mail
Stolen_Computer
Stolen_Computers
Stolen_Documents
Stolen_Laptop
unknown
Web
Confidence Level
Metric
TVaR
VaR


VaR and TVaR by risks at Confidence Levels
75000000
50000000
25000000
0
0.900
0.925
0.950
0.975
Confidence Level
All_Data
HACK
Lost_Tape
Stolen_Computer
Stolen_Laptop
Metric
TVaR
VaR
risks
Email
Lost_Laptop
Lost_Tapes
Stolen_Computers
unknown
Fraud
Lost_Media
Snail_Mail
Stolen_Documents
Web

نتائج الدراسة:

تتمثل أهم النتائج التي توصلت إليها الدراسة فيما يلى:

1) كانت نتائج جودة التوفيق غير ملائمة باستخدام توزيع بواسون لنمذجة أعداد الأخطار السيبرانية لمجموعة البيانات الكاملة (All Data) والمجموعات الفرعية (Biz, Edu, Hack) بسبب التشتت الزائد فى البيانات، ماعدا عدد أخطار (Stolen Laptop) فقد أعطت نتائج جيدة.
2) كانت نتائج جودة التوفيق جيدة ($p>0.05$) باستخدام توزيع ذى الحدين السالب عند نمذجة أعداد الأخطار السيبرانية (All Data, Biz, Edu, Hack, Stolen Laptop) لمعالجة مشكلة التشتت الزائد فى البيانات.
3) أفضلية استخدام توزيع ذى الحدين السالب عن توزيع بواسون عند توفيق البيانات، وذلك لأن توزيع بواسون يفترض أن كلاً من متوسط وتباين البيانات متساويان، وهو ما لا يحدث دائمًا فى البيانات الواقعية.
4) عند نمذجة قيم الأخطار السيبرانية (All Data, Biz, Edu, Hack, Stolen Laptop). أعطت نتائج جيدة مع التوزيع اللوغاريتمى الطبيعى (Log-normal)، بينما كانت غير ملائمة مع توزيع (Skew-normal).
5) سجلت أخطار "Hack, Fraud, Stolen Computer, Lost meida" أعلي قيم لكلاً من VaR و TVaR مقارنة ببقية الأخطار الأخرى عند مستوى ثقة 99.5%، مما يشير إلى أنها أخطار تشكل تهديدًا ماليًا كبيراً. بينما حققت أخطار Email و Lost Laptop قيم VaR و TVaR منخفضة نسبيًا، مما يشير إلى إنخفاض وطأة الخسارة فى هذه الأخطار.
6) كانت المؤسسات التجارية هى الأكثر عرضة للخسائر المالية الكبيرة، بينما حققت المؤسسات الطبية أقل الخسائر.
7) كانت قيم TVaR دائمًا أعلى من قيم VaR لنفس الخطر وكذلك مستوى الثقة، مما يعكس قيمة الخسارة المتوقعة فى أسوأ حالات الخسارة والتى تتخطي قيمة VaR.
8) ثبات قيمة TVaR عند مستوى ثقة معين واستمرار ثباتها عند مستويات الثقة التالية الأعلى، يشير إلى أن قيم الخسائر الكبيرة فى ذيل التوزيع أصبحت مستقرة نسبيا عند هذا المستوى وكذلك المستويات الأعلى.

التوصيات:

توصى الدراسة باستخدام توزيع ذى الحدين السالب عند نمذجة أعداد الأخطار السيبرانية واستخدام التوزيع اللوغاريتمى الطبيعى عند نمذجة قيم الأخطار السيبرانية. وأيضًا توجيه المؤسسات لاستخدام أنظمة الكشف عن الاحتيال والهجمات السيبرانية والوقاية منها، نظرًا لارتفاع قيم VaR و TVaR المرتبطة بكلاً من خطري "Fraud, Hack". كما توصى الدراسة بإجراء مزيد من الدراسات الإكتوارية فى التأمين السيبراني (تأمين أخطار الهجمات الإلكترونية) ومحاولة تسعيره.

المراجع:

أولاً: المراجع العربية:

1) إسماعيل، محمد سعيد (2021): التأمين الإلكترونى ضد الأخطار السيبرانية المشكلات القانونية والحلول المقترحة: دراسة فى القانون القطرى والمقارن، المجلة الدولية للقانون، جامعة قطر - كلية القانون ، المجلد (10)، العدد (3)، ص:204-229.
2) أنجوم، عمر (2021): تحديات مخاطر المنظومات المعلوماتية وأثرها على صناعة التأمين- مجلة الحقوق – الجامعة المستنصرية- كلية القانون- العراق، مج13 ،ع 42، ص:55-78.
3) بدر، صنيه (2021). الأبحاث النوعية فى مراكز الامن السيبراني. المركز العربى للبحوث والدراسات، العدد رقم (69)، ص:12.
4) علم الدين بانقا (2019)، "مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الإقتصادية: دراسة حالة دول مجلس التعاون الخليجى" سلسلة دراسات تنموية – العدد 63، المعهد العربى للتخطيط، الكويت.
5) على، رامز جواد، القحطانى، عادل (2019): التأمين على أخطار الهجمات الإلكترونية، مجلة جامعة البعث للعلوم الإنسانية: جامعة البعث – سوريا (ISSN: 1022-467X)، المجلد (41)، العدد (87)، ص:11-37.
6) نشرة الإتحاد المصرى للتأمين (2019): العدد الأسبوعى رقم 67.

ثانياً: المراجع الأجنبية:

1) Abraham Weishaus (2010): Study Manual for Exam C/Exam 4 - Construction and Evaluation of Actuarial Models -Eleventh Edition.
2) Allianz Global Corporate & Specialty SE “AGCS” (2020): Allianz risk barometer 2020: Identifying the major business risks for 2020. https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020.pdf. Accessed 31 March 2020.
3) Aman Agrawal (2024): Maximum Likelihood Estimation - Parameter Estimation Technique - Machine Learning with Python Code, May 23,2024.
4) Andreas de Vries (2000): The Value at Risk, FH S¨udwestfalen University of Applied Sciences, Haldener Straße 182, D-58095 Hagen, Germany.
5) Bartłomiej BALAWEJDER, Robert DANKIEWICZ, Anna OSTROWSKA DANKIEWICZ, Tomasz TOMCZYK (2019): The role of insurance in cyber risk management in enterprises, Humanities and Social Sciencs, vol. XXIV, 26 (4/2019), P.19-32.
6) Bulgurcu B., H. Cavusoglu, and I. Benbasat (2010): Information security policy compliance: An empirical study of rationality-based beliefs and

information security awareness. Management Information Systems Quarterly 34 (3): 523–548.

7) Cavusoglu H., H. Cavusoglu, and S. Raghunathan (2004): Economics of IT security management: Four improvements to current security practices. Communications of the Association for Information Systems 14: 65–75.

8) Damla Kuru and Sema Bayraktar (2017): The effect of cyber Risk Insurance to Social Welfare. Istanbul Bilgi Universities, Istanbul, Turkey. Journal of Financial Crime, Vol, 24 No. 2, PP329-34

9) Delignette-Muller M. L. and Dutang C. (2015): fitdistrplus: An R Package for Fitting Distributions. Journal of Statistical Software, 64(4), 1–34. https://doi.org/10.18637/jss.v064.i04

10) Denuit, M., Dhaene, J., Goovaerts, M., & Kaas, R. (2005): Actuarial Theory for Dependent Risks: Measures, Orders and Models. John Wiley & Sons.

11) El Bolkiny M., Wasif J.A., Spahr R. W., El Madawye M.M., and Sunderman, M.A. (2018): Estimating the Optimal Proportional Reinsurance Method in Property Insurance, The Egyptian Journal for Commercial Studies, Faculty of Commerce, Mansoura University, Vol. 42, No. 3, 2-24.

12) Eling M. and W. Schnell (2016a): Ten key questions on cyber risk and cyber risk insurance. Zurich: The Geneva Association. https://www.genevaassociation.org/sites/default/fles/research-topics-docum ent-type/pdf_public//cyber-risk-10_key_questions.pdf. Accessed 15 September 2019.

13) Eling M. and W. Schnell (2016b): What do we know about cyber risk and cyber risk insurance?. The Journal of Risk Finance 17 (5): 474–491.

14) Fernanda Figueiredo and M. Ivette Gomes (2011): THE SKEW-NORMAL DISTRIBUTION IN SPC, https://ceaul.org/wp-content/uploads/2018/10/Figueiredo_Gomes_workingpaper.pdf

15) Ganbayar Uuganbayar, Artsiom Yautsiukhin, Fabio Martinellia, Fabio Massacci (2021): Optimization of cyber insurance coverage with selection of cost effective security controls. Computers and Security, https://doi.org/10.1016/j.cose.2020.102121

16) Goulet V. (2007): actuar: An R Package for Actuarial Science, version 0.9-3. École d'actuariat, Université Laval. URL http://www.actuar-project.org

17) Grace Ngunkeng (2013): STATISTICAL ANALYSIS OF SKEW NORMAL DISTRIBUTION AND ITS APPLICATIONS, DOCTOR Dissertation, the Graduate College of Bowling Green State University.

18) Hardy, M. R. (2006): An Introduction to risk Measures for Actuarial Applications. USA: Education and Examination Committee of the Socity of Acturies C-25-07, Casualty Actuarial Society and the Society of Actuaries.

19) Hulisi Ogut Srinivasan R. and Nirup M. (2011): Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self- Protection.Risk Analysis, Vol. 31, No.3.

20) Innerhofer-Oberperfer F. and R. Breu (2010): Potential rating indicators for cyberinsurance: An exploratory qualitative study. In Economics of information security and privacy, ed. T. Moore, D. Pym, and C. Ioannidis, 249–278. Boston, MA: Springer.

21) Jakub Stoklosa, Rachel V. Blakey and Francis K. C. Hui (2022): An Overview of Modern Applications of Negative Binomial Modelling in Ecology and Biodiversity, Diversity 2022, 14, 320, https://doi.org/10.3390/d14050320

22) Järveläinen J. (2013): IT incidents and business impacts: Validating a framework for continuity management in information systems. International Journal of Information Management 33 (3): 583–590.

23) Marco Taboga (2021): "Poisson distribution - Maximum Likelihood Estimation", Lectures on probability theory and mathematical statistics. Kindle Direct Publishing. Online appendix. https://www.statlect.com/fundamentals-of-statistics/Poisson distribution-maximum-likelihood.

24) Maria Francesca Carfora, Fabio Martinelli, Francesco Mercaldo and Albina Orlando (2019): Cyber Risk Management: an actuarial point of view, Journal of operational Risk, Volume 14, Number4.

25) Martin M. Boyer (2020): Cyber insurance demand, Supply, Contracts and cases., published online: 26 August.

26) Natalie M. Scala, Allison C. Reilly, Paul L. Goethals and Michel Cukier (2019): Risk and the five Hard Problems of Cybersecurity. Risk Analysis. Vol. 39, No. 10. 2019.

27) Nor Hasnul Azirah Abdul Hamid, Normalina Ibrahim Mat Nor, Fazlin Marini Hussain, Rajeswari Raju, Humza Naseer and Atif Ahmad (2022).

Barriers and enablers to adoption of cyber insurance in developing countries: An Exploratory study of Malaysian organizations. COMPUTERS & SECURITY | ELSEVIER ADVANCED TECHNOLOGY. DOI: 10.1016/j.cose.2022.102893

28) R Development Core Team (2007): R: A language and environment for statis- tical computing. R Foundation for Statistical Computing, Vienna, Austria. URL http://www.r-project.org

29) Salmela H. (2008): Analyzing business losses caused by information systems risk: A business process analysis approach. Journal of Information Technology 23 (3): 185–202.

30) Smith G. S. (2004): Recognizing and preparing loss estimates from cyber-attacks. Information Systems Security 12 (6): 46–57.

31) Stuart A. Klugman, Harry H. Panjer and Gordon E. Willmot (2019): Loss Models from Data to Decisions, Fifth Edition.

32) Tonn G., J. P. Kesan, L. Zhang, and J. Czajkowski (2019): Cyber risk and insurance for transportation infrastructure. Transport Policy 79: 103–114.

33) Tosh D. K., S. Shetty, S. Sengupta, J. P. Kesan and C. A. Kamhoua (2017): Risk management using cyber-threat information sharing and cyber-insurance. In Game Theory for Networks: 7th International EAI Conference, GameNets 2017, Knoxville, TN, USA, May 9, 2017, Proceedings, ed. L. Duan, A. Sanjab, H. Li, X. Chen, D. Materassi, and R. Elazouzi, 154–164. Cham: Springer.

34) Wendy Hume Hayes (2022): Cyber Insurance and Small Community Banks: A Mixed-Methods Exploration. PhD. Capitol Technology University. August 2022, p iii.

Wikipedia(2023): Negative binomial *distribution*, (https://en.wikipedia.org/wiki/Negative_binomial_distribution)

35) William L. Dunn and J. Kenneth Shultis (2023): Exploring Monte Carlo Methods (Second Edition), https://doi.org/10.1016/B978-0-12-819739-4.00019-6

A Proposed Model for Measuring Cyber Security Risks

Abstract:

This research aims to measure cyber risks (risks of cyberattacks) by modeling the frequency and severity of cyber risks across different risk categories within various institutions using the Poisson distribution, the Negative Binomial distribution, the log-normal distribution, and the Skew-normal distribution. The goal is to fit the distribution and estimate the goodness of fit using the log-likelihood value, the Kolmogorov-Smirnov test value, and the P-value. Additionally, the values of VaR and TVaR were estimated for both the institutions and the various cyber risks. The study revealed that the Negative Binomial distribution performed better than the Poisson distribution in fitting the frequency of risks data. Furthermore, the Log-normal distribution demonstrated a better fit compared to the Skew-normal distribution in fitting the severity of risks data. By estimating the values of VaR and TVaR, the risks of "Hack, Fraud, Stolen Computer, and Lost Media" recorded the highest values for both measures at the 99.5% confidence level, indicating that these risks pose a significant financial threat. On the other hand, the risks of Email and Lost Laptop showed relatively low VaR and TVaR values, suggesting that the severity of losses associated with these risks is lower. The business (BIZ) institutions were found to be the most exposed to significant financial losses, while medical (MED) institutions faced the lowest losses. The study recommended that institutions adopt systems for detecting and preventing fraud and cyberattack risks. Additionally, it suggested conducting further actuarial studies on risks of cyberattacks and pricing insurance policies covering risks of cyberattacks.

Keywords: Cyber Security Risk, cyberattack risks, Skew-normal Distribution, VaR (Value at Risk), TVaR (Tail Value at Risk).