به نام آنکه جانرا فکرت آموخت　　چراغ دل به نور جان بر افروخت
توانا بود هر که دانا بود　　ز دانش دل پیر برنا بود

بانک مرکزی جمهوری اسلامی ایران

دوره آموزشی :

ریسک امنیت اطلاعات در بانکها

(با تکیه بر مدل سازی و تحلیل داده)

مدرس :

سید مرتضی ذکاوت

مرداد ۱۴۰۲

فهرست مطالب

۱. فصل اول :کلیات و تعاریف

۱-۱. مبانی سیستم مدیریت ریسک امنیت اطلاعات مبتنی بر ISO 27002 / ISO 27001

در اقتصاد اطلاعاتی امروزی، توسعه، بهره برداری و حفاظت از اطلاعات و داراییها مرتبط کلید رقابت درازمدت و بقای شرکتها و کل اقتصاد ها است. بنابراین حفاظت از اطلاعات و دارایی های مرتبط یا به عبارت دیگر امنیت اطلاعات ، به عنوان یک مسئولیت اساسی حاکمیت شرکتی از حفاظت از دارایی های فیزیکی پیشی گرفته است. یک سیستم مدیریت امنیت اطلاعات (ISMS)[1] که رویکردی سیستماتیک برای ایجاد، اجرا، عملیات، نظارت، بررسی، حفظ و بهبود امنیت اطلاعات سازمان برای دستیابی به اهداف تجاری را ارائه می کند، در کنار بازاریابی، فروش، منابع انسانی و مدیریت مالی به یک رشته مهم سازمانی تبدیل شده است[2]. یک هدف کلیدی حاکمیت شرکتی حصول اطمینان از این است که سازمان دارای تعادل مناسبی از ریسک و پاداش در عملیات تجاری خود باشد. بر این اساس مدیریت ریسک سازمانی[3] (ERM) به طور فزاینده ای چارچوبی را فراهم می کند که در آن سازمان ها می توانند ریسک ها را در طرح تجاری خود ارزیابی و مدیریت کنند. به رسمیت شناختن ریسک اساسی و استراتژیک در فناوری اطلاعات و ارتباطات منجر به توسعه حاکمیت فناوری اطلاعات شده است.

اقتصاد جهانی در حال تغییر، همراه با پیشرفت‌های اخیر حاکمیت شرکتی و فناوری اطلاعات، همگی زمینه‌ای را فراهم می‌کنند که در آن سازمانها باید ریسک های دارایی‌های اطلاعاتی را که سازمان‌هایشان به آن‌ها وابسته است و تحقق اهداف طرح کسب‌وکارشان، ارزیابی کنند. تصمیمات مدیریت امنیت اطلاعات به طور کامل توسط تصمیمات خاصی که به عنوان نتیجه فرآیند ارزیابی ریسک در رابطه با ریسک های شناسایی شده و دارایی های اطلاعاتی خاص اتخاذ می شود، هدایت می شوند. بنابراین ارزیابی ریسک صلاحیت اصلی مدیریت امنیت اطلاعات است. براساس (ISO 27002) ISO/IEC 27002:2013 ، به عنوان استاندار بین المللی ISMS که رویکرد تجاری و ریسک گرا پشتیبانی را می کند، منابع به کار رفته در اجرای کنترل ها باید در برابر آسیب های تجاری که در غیاب آن کنترل ها ناشی از مسائل امنیتی است، متعادل شوند. نتایج ارزیابی ریسک به عنوان راهنمایی برای تعیین اقدامات مدیریتی و اولویت‌های مناسب برای مدیریت ریسک‌های امنیت اطلاعات و اجرای کنترل‌های انتخاب شده برای محافظت در برابر این خطرات محسوب می شوند. شایان ذکر است که تعداد فزاینده ای از سازمان ها این رویکرد را برای مدیریت ریسک اتخاذ می کنند و برای این منظور تعدادی از استانداردهای ملی یا اختصاصی که با مدیریت ریسک امنیت اطلاعات سروکار دارند در طول سال ها شکل گرفته اند. همه آنها

---

[1]- Information Security Management System (ISMS)

[2] - Calder and Watkins 2019.

[3] - Enterprise Risk Management

اشتراکات زیادی دارند. از جمله ISO 27001 استاندارد بین المللی است که الزامات یک ISMS را تعیین می کند و رویکردی برای مدیریت ریسک مطابق با سایر راهنمایی ها ارائه می دهد. در واقع بسیاری از چارچوب‌های دیگر نیز بر اساس ISO 27001 قابل اجرا هستند. این رویکرد همچنین برای سازمان‌هایی که از استاندارد امنیت داده‌های صنعت کارتهای پرداخت (PCI DSS) پیروی می‌کنند، مناسب است و از انطباق با سایر الزامات قانونی و نظارتی، مانند مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (GDPR) و دستورالعمل امنیت شبکه‌های مستقیم و سیستم‌های اطلاعاتی پشتیبانی می‌کند.

با توجه به این واقعیت که بین سطوح ریسک و پاداش در هر کسب و کاری رابطه وجود دارد هر سازمانی باید معیارهای خود را برای پذیرش ریسک تعیین و سطوح ریسک قابل پذیرش برای خود را شناسایی نماید . بر این اساس اکثر کسب‌وکارها، به‌ویژه آن‌هایی که مشمول قانون ساربانز-آکسلی سال ۲۰۰۲ هستند و در بریتانیا، راهنمای FRC در مورد مدیریت ریسک، کنترل داخلی و گزارش‌های مالی و تجاری مرتبط و قانون حاکمیت شرکتی بریتانیا، باید مشخص نمایند که چه ریسک‌هایی که می‌پذیرند و کدام‌ها را نمی‌پذیرند، و میزان و چگونگی ریسک های مورد پذیرش را نیز تعیین نمایند. بدین منظور لازم است رویکرد مزبور برای مدیریت خطوط کسب و کار طور کلی و خاص مشخص شود. همانطور که اشاره شد، ارزیابی ریسک، به عنوان یک فعالیت، باید در چارچوب چارچوب ERM گسترده‌تر سازمان مورد بررسی قرار گیرد.

در اغلب موارد، سازمان ها بدون در نظر گرفتن اینکه این عمل باید بخشی از یک طرح بزرگتر باشد، وارد مدیریت ریسک می شوند. لازم به ذکر است که ارزیابی ریسک به خودی خود یک هدف نیست: ارزیابی ریسک باید خروجی هایی را ارائه دهد که برای سازمان مفید باشد. هدف یک روش ارزیابی ریسک باید تأثیرگذاری بر ISMS سازمان باشد. در حالی که ISO 27002 یک مبنا و استاندارد عملی است، ISO) ISO/IEC 27001:2013 (27001 مشخصاتی است که الزامات یک ISMS را تعیین می کند. ISO 27001 به صراحت این الزام را دارد که از ارزیابی ریسک امنیت اطلاعات برای اطلاع از انتخاب کنترل ها به کار گرفته شود.

سازمان هایی که یک ISMS را مطابق با ISO 27001 طراحی و اجرا می کنند، می توانند آن را توسط یک مرجع صدور گواهینامه شخص ثالث ارزیابی کنند و اگر پس از بررسی، مطابقت با ISO 27001 تشخیص داده شود، گواهی انطباق معتبر می تواند صادر شود.

این استاندارد به طور فزاینده ای به عنوان ارائه راه حلی عملی برای گستره رو به رشد الزامات نظارتی مرتبط با اطلاعات و همچنین کمک به سازمان ها برای مقابله مقرون به صرفه تر با طیف فزاینده پیچیده و متنوع تهدیدات امنیت اطلاعات در اقتصاد اطلاعاتی مدرن تلقی می شود. به امنیت اطلاعات

یک ISMS توسعه یافته و بر اساس معیارهای پذیرش ریسک، و استفاده از گواهینامه معتبر شخص ثالث برای ارائه تأیید مستقل از سطح اطمینان، یک ابزار مدیریتی بسیار مفید است. چنین ISMS فرصتی را برای تعریف و نظارت بر سطوح خدمات در داخل، و همچنین در سازمان‌های پیمانکار/شریک ارائه می‌دهد، بنابراین میزان کنترل مؤثر ریسک‌هایی را که مدیران و مدیریت ارشد نسبت به آنها پاسخگو هستند، نشان می‌دهد.

به طور فزاینده ای رایج می شود که گواهینامه ISO 27001 یک پیش نیاز در اسناد تدارکات مشخصات خدمات باشد و از آنجایی که خریداران در درک خود از طرح صدور گواهینامه معتبر ISO 27001 پیچیده تر می شوند، بنابراین آنها به طور فزاینده ای الزامات خود را به طور خاص تر، نه تنها از نظر خود گواهینامه و همچنین از نظر سطح گواهینامه، بلکه با توجه به سطح مورد نیاز برای گواهینامه تعیین می کنند. این بلوغ سریع در درک خریداران، سازمان ها را به سمت بهبود کیفیت ISMS خود سوق می دهد.

البته سطح اطمینان مستقیماً به ارزیابی ریسک و جنبه های مدیریتی ایجاد و نگهداری ISMS مطابق با ISO 27001 مربوط می شود. این جنبه کلیدی است که تضمین می کند که یک سطح ثابت از اطمینان در تمام جنبه های امنیت اطلاعات در یک سازمان به دست می آید.

ISO 27001 مشخصات یک ISMS است. همانطور که گفتیم بر اساس ارزیابی ریسک، هم در ابتدا و هم به صورت مستمر است. ISO 27001 تا آنجا پیش می رود که الزاماتی را که یک رویکرد مدیریت ریسک امنیت اطلاعات باید برآورده کند، مشخص می کند. در حالی که بسیاری از رویکردهای شناخته شده و معتبر برای ارزیابی ریسک وجود دارد، سازمانی که مایل به دریافت گواهینامه ISO 27001 است باید الزامات تعیین شده در خود استاندارد را برآورده کند. جایی برای اقدامات نیمه وجود ندارد: یا یک روش ارزیابی ریسک مطابق با الزامات ISO 27001 است، در این صورت صدور گواهینامه معتبر در دسترس است، یا چنین نیست، در این صورت صدور گواهینامه معتبر قابل دستیابی نیست.

این کتاب برای گسترش راهنمایی هایی نوشته شده است که قبلاً در سایر کتاب های پیاده سازی ISO 27001 توسط همان نویسندگان موجود است. این برگرفته از بهترین رویه ملی و بین‌المللی نوظهور در مورد ارزیابی ریسک است، از جمله استاندارد بریتانیا (BS 7799-3) BS 7799-3:2017، که برای همسویی با نسخه ۲۰۱۳ ISO 27001 منتشر شده است. همچنین برای ارائه راهنمایی‌های دقیق و عملی به تیم‌های امنیت اطلاعات و مدیریت ریسک در مورد چگونگی توسعه و اجرای یک ارزیابی ریسک در راستای فرآیند ISO7 نوشته شده است. بهترین راهنمای عملی BS 7799-3، و به طور همزمان مزایای تجاری واقعی و نهایی را ارائه می دهد.

مدیریت ریسک

NIST می‌گوید: «ریسک» «اندازه‌گیری میزانی است که یک موجودیت توسط یک موقعیت یا رویداد بالقوه تهدید می‌شود، و معمولاً تابعی از موارد زیر است:

- تأثیر نامطلوبی که در صورت وقوع شرایط یا رویداد ایجاد می‌شود
- احتمال وقوع

استاندارد "ISO/IEC 27000:2018 در خصوص سیستم های مدیریت امنیت اطلاعات ریسک را به عنوان اثر عدم قطعیت بر اهداف تعریف می کند، با یک یادداشت فرعی که بیان می کند که "ریسک اغلب به صورت ترکیبی از تغییرات مرتبط با شرایط و پیامدهای مرتبط بیان می شود". تعریف NIST از ریسک مطابق با تعریفی است که در ISO 27000 استفاده شده است و اولین شاخصی است که ارزیابی ریسک که الزامات ISO 27001 را برآورده می کند نیز مطابق با توصیه های NIST است. تفاوت اصلی بین تعاریف NIST و ISO 27000 در این است که دومی احتمال خطرات دارای پیامدهای مثبت را در بر می گیرد. با این حال، ISO 27000 یک یادداشت دیگر دارد که «ریسک امنیت اطلاعات با این پتانسیل همراه است که تهدیدها از آسیب‌پذیری‌های یک دارایی اطلاعاتی یا گروهی از دارایی‌های اطلاعاتی سوء استفاده کرده و در نتیجه به سازمان آسیب وارد می‌کنند» که تمرکز بر خطرات دارایی‌های اطلاعاتی منعکس‌شده در نسخه‌های قبلی خانواده ISO 27000 را حفظ می‌کند و در عین حال می‌تواند منجر به آسیب‌پذیری از استانداردها شود.

BS 7799-3 برای تعاریف خود به ISO 27000 اشاره می کند و راهنمای آن بر این اساس ارائه شده است.

همه سازمان‌ها روزانه با خطراتی از یک نوع مواجه هستند و ISO 27001 انتظار دارد که خط‌مشی مدیریت امنیت اطلاعات سازمان با جهت استراتژیک سازمان» همسو بوده و «مناسب با هدف سازمان باشد.

مدیریت ریسک: دو مرحله

مدیریت ریسک فرآیندی است که به مدیران اجازه می‌دهد تا هزینه‌های عملیاتی و اقتصادی اقدامات حفاظتی را متعادل کنند و با حفاظت از سیستم‌های فناوری اطلاعات و داده‌هایی که مأموریت‌های سازمانشان را پشتیبانی می‌کنند، به دستاوردهایی در قابلیت مأموریت دست یابند.

سازمان‌ها استراتژی‌های مدیریت ریسک را به منظور کاهش اثرات منفی و ایجاد مبنایی ساختاریافته و ثابت برای تصمیم‌گیری در مورد گزینه‌های کاهش ریسک، توسعه و اجرا می‌کنند. برای در نظر گرفتن مبحث مدیریت ریسک، دارای دو فاز ارزیابی ریسک و درمان ریسک است، اما در عمل یک فعالیت مستمر است که شامل اسکن افق، ارزیابی ریسک، تصمیم‌گیری ریسک، درمان(های) ریسک، ارتباط، ارزیابی مجدد، درمان‌های بعدی و غیره می‌شود. ارزیابی ریسک فرآیند شناسایی و برآورد ریسک هایی است که سازمان ممکن است در معرض آن قرار گیرد.

درمان ریسک فرآیند پاسخگویی به ریسک های شناسایی شده در پرتو تصمیمات ریسک است.

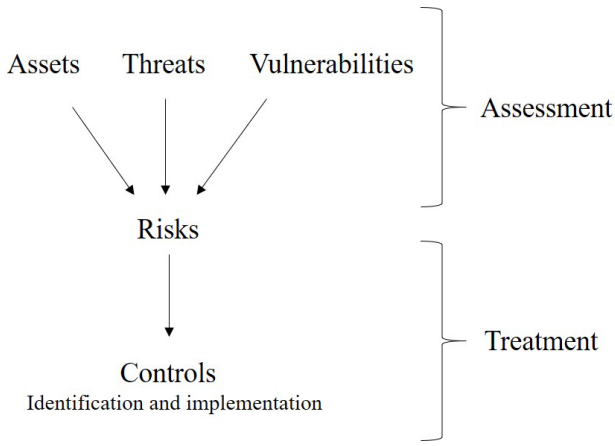
ارزیابی ریسک معمولاً یکی از دو روش زیر را اتخاذ می کند:

• فرآیند شناسایی سناریوها، تأثیر آنها بر سازمان و دفعات وقوع آنها.

• تمرکز بر دارایی های اطلاعاتی و تهدیداتی که آنها در معرض آن هستند. در نظر گرفتن آسیب‌پذیری‌هایی که تهدیدها ممکن است از آنها سوء استفاده کنند، ارزیاب ریسک را قادر می‌سازد تا احتمال و تأثیر هر ریسک شناسایی‌شده را شناسایی کند.

در توضیح ساده دو مرحله ای مدیریت ریسک، مرحله ارزیابی ریسک سپس به مرحله درمان ریسک منتهی می شود. هر تصمیم و/یا اقدامی که در پرتو ارزیابی ریسک انجام می‌شود، خارج از فرآیند ارزیابی ریسک اتخاذ می‌شود و بخشی از فعالیت برنامه‌ریزی درمان ریسک است که همراه با فرآیند ارزیابی ریسک، جزء دیگر مدیریت ریسک است. مدیریت ریسک ابرمجموعه ارزیابی ریسک است و بنابراین شامل ارزیابی ریسک می شود.

ارزیابی ریسک و درمان ریسک دو فرآیند فرعی مدیریت ریسک هستند که در رابطه با ارزیابی مبتنی بر دارایی در شکل ۱ مشاهده می شود.



شکل ۱- چارچوب مدیریت ریسک

۲-۱. نیاز به اطمینان از اطلاعات[1]

دارایی‌های اطلاعاتی و زیرساخت‌های سازمان‌ها دائماً مورد تهدید قرار می گیرند. محیط تهدید پویا نیاز به اطمینان از اطلاعات را افزایش داده است. اطمینان از اطلاعات فقط یک موضوع فناوری نیست، بلکه یک موضوع تجاری و اجتماعی نیز هست. در نهایت، هدف اطمینان از اطلاعات، حفاظت از اطلاعات و زیرساخت هایی است که از

[1] - Information Assurance

ماموریت و چشم انداز سازمان از طریق رعایت مقررات، مدیریت ریسک و سیاست های سازمانی پشتیبانی می کند. یک اصطلاح مرتبط، فناوری اطلاعات، بر پردازش، ذخیره سازی، اطمینان از در دسترس بودن و به اشتراک گذاری دارایی های اطلاعاتی تمرکز دارد. چگونه اطمینان از اطلاعات با این مشکلات مقابله می کند؟ اطمینان از اطلاعات شامل محافظت از اطلاعات و خدمات در برابر افشا، انتقال، اصلاح یا تخریب (اعم از عمدی یا غیرعمدی) و اطمینان از در دسترس بودن اطلاعات به موقع است. اطمینان از اطلاعات همچنین احراز هویت مورد استفاده در یک سیستم و اینکه چقدر اقدامات را می توان به شدت رد کرد، در نظر می گیرد. اساساً تضمین می‌کند که تنها نهادهای تأیید شده اطلاعات دقیق مورد نیاز خود را در صورت نیاز دریافت می‌کنند. ایمن سازی اطلاعات با اجرای کنترل های مناسب و مقرون به صرفه تضمین می کند که دارایی های اطلاعات حساس و حیاتی به اندازه کافی محافظت می شوند. برای موفقیت، ارزیابی حساسیت و بحرانی بودن برنامه ها و داده ها و همچنین سطح ریسک قابل قبول سازمان برای سازمان ها حیاتی است. همانطور که در چندین سال گذشته گزارش‌های بررسی نقض داده‌های Verizon نشان داده شده است، برای مشاهده تجاوز مداوم به استفاده از فناوری اطلاعات سازمان‌ها در سراسر جهان، فقط باید اخبار را بخوانید. به عنوان یک بخش اساسی از انجام کسب و کار، سازمان ها باید دارایی های اطلاعاتی خود را فهرست بندی کرده و آنها را در برابر تهدیدات و آسیب پذیری ها ارزیابی کنند. ارزیابی باید شامل اطلاعات مشتری، ایمیل، اطلاعات مالی، منابع برنامه، رسانه های اجتماعی، ترتیبات برون سپاری و استفاده از فناوری‌های رایانش ابری باشد. متعاقباً، سازمان باید کنترل‌های امنیتی را برای حفاظت از دارایی‌های اطلاعاتی با هزینه‌ای قابل قبول به کار گیرد.

۳-۱. اصول اطمینان از اطلاعات

هنگامی که اهمیت اطمینان از اطلاعات را درک کردید، باید برخی از انتظارات اساسی را قبل و در طول اجرای امنیت، مستقل از اندازه یا ماهیت کسب و کار، بپذیرید. اگر سازمانی بخواهد به زبان ریسک مشترک صحبت کند و اهداف مشترک را درک کند، یک مدل مشترک و درک اطمینان از اطلاعات ضروری است. مدل اطمینان از اطلاعات مورد استفاده در این کار، مدل (MSR)[1] است. سه اقدام متقابل ضروری (فناوری، سیاست و مردم)؛ و پنج سرویس اساسی (در دسترس بودن، یکپارچگی، احراز هویت، محرمانه بودن، و عدم انکار). انجمن شناخته شده بین المللی ماشین های محاسباتی[2] (ACM) این را به عنوان توسعه ای از مدل اولیه محرمانگی، یکپارچگی و در دسترس بودن[3] (CIA) و توسعه کار جان مک کامبر در اوایل دهه ۱۹۹۰ پذیرفت.

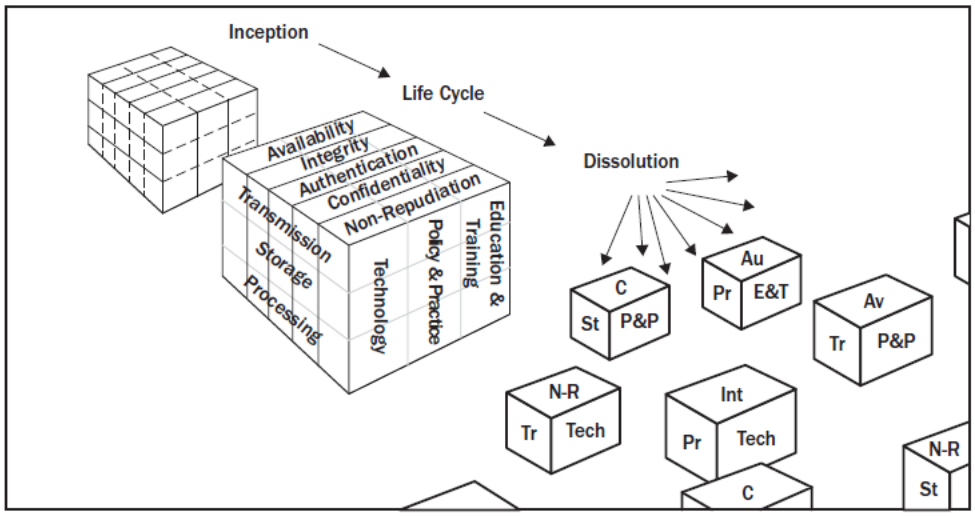
[1] - Maconachy, Schou, Ragsdale
[2] - Association for Computing Machines
[3] - Confidentiality, Integrity, Availability

ما انتظارات اساسی و باورهای مشترکی را که طی سال‌ها از طریق فعالیت‌های تجاری به دست آمده‌اند، شناسایی کرده‌ایم و در اینجا به آنها به عنوان اصول اطمینان از اطلاعات اشاره می‌کنیم. هفت اصل مشخص می کند که اطمینان از اطلاعات باید شامل موارد زیر باشد:

- توانمندساز کسب و کار باشند
- از عنصر اتصال سیستم های یک سازمان محافظت نمایند
- مقرون به صرفه و مقرون به صرفه باشد
- ایجاد مسئولیت و پاسخگویی نماید
- در پی روش قوی و پایدار[1] باشند
- به صورت دوره ای ارزیابی شوند
- محدود به تعهدات اجتماعی باشند

مدل MSR را می توان در شکل به صورت شماتیک در نظر گرفت :

شکل ۱ – مدل شماتیک MSR



مأخذ: (Hernandez and Schou 2014,p.14)

این هفت اصل شما را قادر می سازد تا مدل MSR نشان داده شده در شکل ۱ را پیاده سازی کنید. مدل MSR خدمات امنیتی، ایالت ها و اقدامات متقابل را مشخص می کند، همانطور که قبلا توضیح داده شد. علاوه بر این، این مدل رابطه درهم تنیده بین این ۴۵ ترکیب منحصر به فرد را نشان می دهد. این ایده را تقویت می کند که مدیریت ارشد و مدیران ارشد مسئول چرخه حیات سیستم و اطلاعات یک سازمان از آغاز تا انحلال هستند. درک

[1] - Rubost

تمایز بین اصطلاحات زیر برای شناسایی نه تنها فضای بازار، بلکه مفاهیم اساسی در حفاظت از دارایی های اطلاعاتی سازمان ها بسیار مهم است:

- اطمینان از اطلاعات
- امنیت اطلاعات
- حفاظت از اطلاعات
- امنیت سایبری

در ادامه هر کدام از مؤلفه های فوق را تعریف می نماییم.

- اطمینان از اطلاعات

اطمینان از اطلاعات رویکردی فراگیر برای شناسایی، درک و مدیریت ریسک از طریق استفاده سازمان از اطلاعات و سیستم های اطلاعاتی است. همانطور که در مدل MSR اشاره شد، اطمینان از اطلاعات به چرخه عمر اطلاعات در یک سازمان از طریق اهداف حفظ خدمات یا ویژگی های زیر مربوط می شود:

- محرمانه بودن
- تمامیت
- دسترسی
- عدم انکار
- احراز هویت

موارد زیر عناصر مهمی هستند که باید در مورد اطمینان از اطلاعات به خاطر بسپارید:

- ✓ اطمینان از اطلاعات شامل تمام اطلاعاتی است که یک سازمان ممکن است بدون توجه به رسانه پردازش، ذخیره، انتقال یا انتشار دهد. بنابراین، اطلاعات روی کاغذ، روی هارد دیسک، در ذهن یک کارمند یا در فضای ابری "در محدوده" در نظر گرفته می شود.
- ✓ امنیت اطلاعات، حفاظت از اطلاعات و امنیت سایبری زیرمجموعه های اطمینان از اطلاعات هستند.

- امنیت اطلاعات

امنیت اطلاعات یک زیر دامنه اطمینان از اطلاعات است. همانطور که در مدل MSR اشاره شد، امنیت اطلاعات بر سه گانه زیر تمرکز دارد.

- محرمانه بودن
- تمامیت
- دسترسی

موارد زیر عناصر مهمی هستند که باید در مورد امنیت اطلاعات به خاطر بسپارید:

- ✓ مانند اطمینان از اطلاعات، امنیت اطلاعات شامل تمامی اطلاعات می باشد. سازمان ممکن است بدون توجه به رسانه پردازش، ذخیره، انتقال یا انتشار دهد. بنابراین، اطلاعات روی کاغذ، روی هارد دیسک، در ذهن یک کارمند یا در فضای ابری در محدوده مورد توجه قرار می گیرد.
- ✓ حفاظت از اطلاعات و امنیت سایبری زیرمجموعه های امنیت اطلاعات هستند.

➢ حفاظت از اطلاعات

حفاظت از اطلاعات بهتر است به عنوان زیرمجموعه ای از امنیت اطلاعات در نظر گرفته شود. اغلب بر حسب حفاظت از محرمانه بودن و یکپارچگی اطلاعات از طریق ابزارهای مختلفی مانند خط مشی، استانداردها، کنترل های فیزیکی، کنترل های فنی، نظارت و طبقه بندی یا طبقه بندی اطلاعات تعریف می شود. موارد زیر عناصر مهمی هستند که باید در مورد حفاظت از اطلاعات به خاطر بسپارید:

- ✓ مانند امنیت اطلاعات، حفاظت از اطلاعات شامل تمام اطلاعاتی است که سازمان ممکن است بدون توجه به رسانه پردازش، ذخیره، انتقال یا انتشار دهد. بنابراین، اطلاعات روی کاغذ، روی هارد دیسک، در ذهن یک کارمند یا در فضای ابری در محدوده مورد توجه قرار می گیرد.
- ✓ برخی از قوانین، مقررات و قوانین به طور خاص حفاظت از اطلاعات را به عنوان یک الزام برای اطلاعات حساس مانند اطلاعات قابل شناسایی شخصی و اطلاعات سلامت شخصی ذکر می کنند.

➢ امنیت سایبری

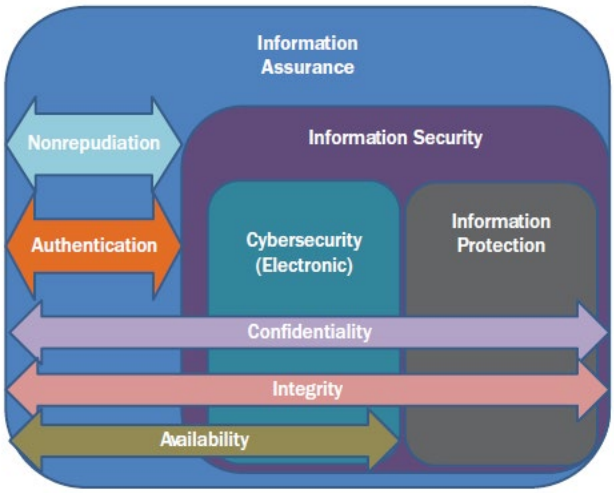
امنیت سایبری یک اصطلاح نسبتاً جدید است که تا حد زیادی جایگزین واژه امنیت رایانه شده است. این اصطلاح اغلب با اطمینان از اطلاعات و امنیت اطلاعات اشتباه گرفته می شود. امنیت سایبری برای توصیف اقدامات انجام شده برای محافظت از سیستم های اطلاعات الکترونیکی در برابر دسترسی یا حمله غیرمجاز استفاده می شود. امنیت سایبری در درجه اول با همان اهداف امنیت اطلاعات در محدوده سیا سیستم های اطلاعات الکترونیکی مرتبط است.

موارد زیر عناصر مهمی هستند که باید در مورد امنیت سایبری به خاطر بسپارید:

- ✓ امنیت سایبری در درجه اول بر حفاظت از شبکه ها و سیستم های اطلاعات الکترونیکی متمرکز است. سایر رسانه ها مانند کاغذ، پرسنل و در برخی موارد سیستم های مستقل که بر امنیت فیزیکی متکی هستند، اغلب خارج از محدوده امنیت سایبری هستند.

- ✓ امنیت سایبری اغلب بر روی آسیب پذیری ها و تهدیدات یک سیستم اطلاعاتی در سطح تاکتیکی تمرکز می کند. اسکن سیستم، اصلاح کردن، و اجرای پیکر بندی ایمن از کانون های رایج امنیت سایبری هستند.
- ✓ تشخیص نفوذ و پاسخ به حادثه و سایر عملکردهای که معمولاً از یک مرکز عملیات امنیتی[1] (SOC) اجرا می شوند اغلب به عنوان عملکردهای امنیت سایبری شناسایی می شوند. شکل ۲ رابطه بین حفاظت اطلاعات، امنیت سایبری، امنیت اطلاعات و اطمینان از اطلاعات و رابطه آنها با محرمانه بودن، یکپارچگی، در دسترس بودن و عدم انکار را نشان می دهد.

شکل ۲- اطمینان از اطلاعات و زیر دامنه های آن



مأخذ: (Hernandez and Schou 2014,p.16)

۱-۴. اهمیت مدیریت ریسک امنیت اطلاعات در بانکها

مدیریت ریسک مبنای اساسی در فرآیندهای تصمیم گیری بسیاری از سازمان ها است. با این حال، مدیریت ریسک امنیت اطلاعات گاهی اوقات می تواند کنار گذاشته شود. اگرچه این فقط در مورد فناوری اطلاعات نیست، مدیریت ریسک سایبری یکی از مهم ترین خطرات است و پیامدهای تجاری پشت هر حادثه امنیت سایبری است. به این معنا که مدیریت ریسک امنیت اطلاعات یک فرآیند مهم برای همه نوع و اندازه سازمان است. اجرای مدیریت ریسک موثر به سازمان ها اجازه می دهد تا به اهداف خود کمک کنند و علاوه بر آن استراتژی های امنیتی خود را تعریف کنند.

۱-۵. امنیت اطلاعات در مقابل امنیت سایبری

[1] - Security Operation Center

به راحتی می توان امنیت اطلاعات و امنیت سایبری را اشتباه گرفت، زیرا این دو حوزه از بسیاری جهات با هم همپوشانی دارند. در واقع همچنانکه ذکر شد امنیت سایبری زیرمجموعه ای از امنیت اطلاعات است. با این حال، این دو رشته های کاملاً یکسانی نیستند و هر کدام دارای تخصص های مجزا بوده و به مجموعه مهارت های متفاوتی نیاز دارند. برای این منظور در ادامه شباهت ها و تفاوت های بین امنیت اطلاعات و امنیت سایبری، تبیین می شود.

موسسه ملی استاندارد و فناوری (NIST)[1] امنیت اطلاعات و امنیت سایبری را به عنوان حوزه های شغلی جداگانه می شناسد. همانطور که گفته شد، مطمئناً بین این دو همپوشانی وجود دارد. در زیر تعاریف و تمایزات کلیدی هر کدام آورده شده است.

۱-۵-۱. امنیت اطلاعات چیست؟

تا حدودی، تقریباً همه مایلند که اطلاعات شخصی آنها ایمن باشد، به این معنی که فقط افراد مجاز می توانند به آنها دسترسی داشته باشند و از آنها استفاده کنند. این هدف امنیت اطلاعات (infosec) است. طبق NIST، infosec شامل محافظت از اطلاعات و سیستم های اطلاعاتی در برابر استفاده غیرمجاز است. هدف این رشته در دسترس بودن، یکپارچگی و محرمانه بودن اطلاعات است. یکی از راه‌های درک infosec در مقایسه با امنیت سایبری این است که این فیلد را به‌عنوان یک چتری ببینیم که شامل همه داده‌ها می‌شود، نه فقط داده‌های ذخیره شده در فضای سایبری. این نشان می دهد که چگونه امنیت سایبری نوعی امنیت اطلاعات است، اما این دو زمینه یکسان نیستند. تیم های امنیت اطلاعات سیاست ها و سیستم هایی را برای حفاظت از اطلاعات ایجاد و اجرا می کنند. برای سازمان های بزرگ، سیستم های امنیتی سختگیرانه برای محافظت از مشتریان مورد نیاز است.

۲-۵-۱. امنیت سایبری چیست؟

زندگی در قرن بیست و یکم به این معنی است که بسیاری از داده ها در سیستم ها و شبکه های کامپیوتری ذخیره می شوند. این مورد تقریباً برای هر صنعتی مصداق دارد از این رو اطلاعات باید تا حد زیادی محافظت شوند. متخصصان امنیت اطلاعات با تمرکز بر امنیت سایبری مسئول ایمن سازی این داده ها هستند. NIST امنیت سایبری را محافظت، جلوگیری از آسیب و بازیابی خدمات و سیستم های ارتباطات الکترونیکی تعریف می کند. این شامل اطلاعات ذخیره شده در این سیستم ها می شود که متخصصان امنیت سایبری برای محافظت از آنها تلاش می کنند. امنیت سایبری همه چیزهایی را که با سیستمهای الکترونیکی و ارتباطات مرتبط است، پوشش می‌دهد.

[1]- National Institute of Standards and Technology

در حوزه امنیت سایبری زیرمجموعه هایی وجود دارد که مستلزم تخصص بیشتر است. اینها شامل امنیت فضای ابری، شبکه و زیرساخت های حیاتی است.

۳-۵-۱. عمده ترین تفاوت های امنیت اطلاعات و امنیت سایبری

سردرگمی بین امنیت اطلاعات و امنیت سایبری ممکن است رخ دهد زیرا بسیاری از اطلاعاتی که ما می خواهیم ذخیره، محافظت و انتقال دهیم در فضای سایبری وجود دارد. در حالی که امنیت سایبری بخشی از امنیت اطلاعات است، جنبه های خاصی از امنیت اطلاعات در حوزه امنیت سایبری گنجانده نشده است. امنیت اطلاعات اصطلاحی فراگیر برای ایجاد و نگهداری سیستم ها و سیاست هایی برای محافظت از هر گونه اطلاعات اعم از دیجیتالی، فیزیکی یا معنوی، نه فقط داده ها در فضای سایبری است. یک کارشناس امنیت اطلاعات ممکن است ابزار دسترسی به داده ها توسط افراد مجاز را توسعه دهد یا اقدامات امنیتی را برای ایمن نگه داشتن اطلاعات ایجاد کند. از سوی دیگر، امنیت سایبری بر محافظت از اطلاعات در برابر حملات سایبری مانند باج افزار و جاسوس افزار تمرکز دارد.

۴-۵-۱. چگونه امنیت اطلاعات و امنیت سایبری همپوشانی دارند

امنیت اطلاعات و امنیت سایبری از بسیاری جهات همپوشانی دارند. این رشته ها علاوه بر داشتن شیوه های امنیتی مشابه، به آموزش و مهارت های مشابه نیز نیاز دارند. بدین منظور شیوه های امنیتی مشترک این دو به شرح ادامه می باشد.

مهم ترین همپوشانی بین infosec و امنیت سایبری این است که آنها از مدل سه گانه CIA[1] (محرمانه بودن، یکپارچگی و در دسترس بودن اطلاعات) برای توسعه سیاست های امنیتی استفاده می کنند.

اولین مورد از سه گانه مزبور محرمانگی است، کی طی آن اطمینان حاصل می شود که اطلاعات فقط توسط کاربران مجاز قابل دسترسی و تغییر باشد. به عنوان مثال، از دیدگاه مصرف کننده، ما از خرده فروشان آنلاین انتظار داریم که داده های ما مانند اطلاعات کارت اعتباری، آدرس خانه و سایر اطلاعات شخصی را ذخیره و محافظت کنند. دوم، یکپارچگی اطلاعات تضمین می کند که اطلاعات دستکاری نشده و کاملا قابل اعتماد باشد. در مثال خرده‌فروش آنلاین این بدین معنی است که داده‌های ارسال شده بین خرده‌فروش و بانک باید ایمن باشند. در غیر این صورت ممکن است بین هزینه واقعی کالای شما و مبلغی که پرداخت کرده اید مغایرت وجود داشته باشد. در نهایت، در دسترس بودن اطلاعات به این معنی است که داده ها در صورت نیاز در دسترس هستند.

---

[1]- Confidentiality, Integrity and Availability of information (CIA)

برای مثال، اگر نیاز دارید که بدانید چقدر پول در حساب بانکی خود دارید، باید بتوانید به آن اطلاعات دسترسی داشته باشید.

۲. فصل دوم : مدیریت ریسک امنیت سایبری در موسسات مالی

اگر جرایم سایبری با سایر شرکت های مجرمانه جهانی مقایسه شود، از نظر هزینه به عنوان درصدی از تولید ناخالص داخلی جهانی (GDP) رتبه چهارم را از بین پنج جنایت پر تاثیر قرار می دهد. تنها جرایم فراملی (۱.۲ درصد)، مواد مخدر (۰.۹ درصد) و جعل/ سرقت اطلاعات (۰.۸۹ درصد) از نظر تأثیر مالی در رتبه بالاتری قرار دارند. با این حال، طبق مطالعه‌ای که در سال ۲۰۱۴ توسط مرکز مطالعات استراتژیک و بین‌المللی انجام شد، جرایم سایبری به سمت بالاترین سطح حرکت می‌کند و ۰.۸ درصد از تولید ناخالص داخلی جهانی را تشکیل می‌دهد[1]. در حالی که بسیاری ممکن است از هزینه جهانی جرایم سایبری آگاه نباشند، شرکت ها در همه جا مطمئناً عواقب نفوذ و سازش را احساس می کنند به نحوی که اثرات این جرایم خالص درآمد شرکت را تحت تأثیر جدی قرار داده است. جرایم سایبری نیز مورد توجه قانونگذاران، بانک های مرکزی و ناظرین مالی همچنین هیأت مدیر شرکت ها قرار گرفته است چرا که گزارش های نفوذ و عواقب آن به صورت روزانه منتشر می شود. همه به طور نگران کننده ای از جرایم سایبری آگاه می شوند، همانطور که دائماً در اخبار است. از سوی دیگر جرایم سایبری نیز می تواند بسیار شخصی باشد و اشخاص را به طور مستقیم درگیرنماید. زیرا احتمالاً که هر یک از ما ممکن است تجربه دریافت اعلان هایی را داشته ایم که اطلاعات مالی و سایر اطلاعات شخصی در یک حمله به خطر افتاده باشد. از سوی دیگر وقوع جرایم سایبری می تواند به طور جدی اعتماد عمومی را نیز از بین ببرد.

۱-۲. اهمیت مدیریت ریسک امنیت در محیط سایبری

صنعت مالی به ارتباط بین مؤسسات، بازارها، ارائه دهندگان خدمات و مشتریانی بستگی دارد که به یک محیط فناوری بسیار پیچیده متکی هستند. ویژگی‌های در حال تحول معماری سیستم‌های مالی جهانی موجب گسترش مجموعه‌ای از چالش‌های مدیریتی شده است. ریسک امنیت سایبری در سرتاسر معماری سازمانی در حوزه‌های فناوری، پرسنل و فرآیند وجود دارد که منجر به چالش‌های مدیریت ریسک اساسی می‌شود. انواع تهدیدها مشهود

[1] - Antonucci 2017.

هستند و می توانند از بسیاری از جنبه های پیچیدگی جدید موجبات سوء استفاده از طریق دسترسی به سیستم های حیاتی و اطلاعات حساس شوند. در این فصل به طور اجمالی ماهیت و گستره تهدیدات رایج امنیت سایبری بر موسسات و بازارهای مالی بررسی می شود. ما شاهد یک پدیده واقعاً جهانی هستیم که خود را به چندین شکل نشان داده است. آشکار است که سطح نسبی مهارت و انگیزه دشمنان طی چند سال گذشته به طور قابل توجهی بهبود یافته است و درجه پیچیدگی حملات همچنان رو به رشد است. تاکتیک های مهاجم با اشکال متوالی حملات که اغلب بر روی بردارهای حمله قبلی بهبود می یابند تکامل سریعی داشته است. براین اساس شناخت و دانش دقیق از تهدیدات غالب برای توسعه موثر معماری امنیت سایبری موثر ضروری است. این دانش باید شامل درک انواع مختلف عوامل تهدید و انگیزه های مربوط به آنها و همچنین تاکتیک های رایج باشد. فهم و درک دقیق تهدیدات نه تنها برای دفاع در برابر آنها، بلکه برای طرح توجیهی به منظور تأمین بودجه دفاعی کافی ضروری است. درک عمیق تهدیدات امنیت سایبری واقعی که بر مؤسسات تأثیر می گذارند باید با رهبران کسب و کار به اشتراک گذاشته شود تا از تصمیمات تخصیص منابع پشتیبانی و راهنمایی شود. شایان ذکر است برخی از راه حل های امنیتی که توسط تأمین کنندگاه ارائه می شود، گاهی باعث افزایش ترس، عدم اطمینان و شک در تلاش برای فروش محصولات و خدمات به بازار امنیت سایبری شده که می تواند منجر به شک و تردیدهای بزرگ از سوی رهبران تجاری شود. تسلط بر مفاهیم تهدید، و نظارت مستمر از چشم انداز تهدید، ممکن است مدیران را متقاعد کند که تهدید فعلی واقعیت داشته و نیاز به پاسخ مناسب دارد.

۲-۲. ریسک امنیت سایبری به عنوان ریسک عملیاتی

تهدیدهای سایبری سازمان را به عنوان ریسک عملیاتی تحت تأثیر قرار می دهند – خطری که به طور بالقوه ناشی از شکست های کنترلی در هر یک از آنها است یا بر آنها تأثیر می گذارد. حوزه معماری سازمانی به طور بالقوه می تواند فرصتهایی را برای اختلالات اعم از عمدی یا غیرعمدی ناشی از سیستم ها و فرآیندهای ناموفق بوجود آورد. ریسک عملیاتی در همه سیستم‌ها، فرآیندها و فعالیت‌های مالی وجود دارد و در نهایت می‌تواند منجر به رویدادهای مالی و سایر انواع ریسک شود. انتظار می رود که مدیریت سازمانی بستری را برای درمان جنبه های مختلف ریسک عملیاتی فراهم کند. با این حال، ریسک امنیت سایبری ویژگی های نسبتاً منحصر به فردی دارد که آن را از انواع دیگر چالش های عملیاتی متمایز می کند. در صنعت مالی، ریسک عملیاتی معمولاً به طور مستقیم و غیرمستقیم شامل فناوری می شود. خطرات مستقیم شامل احتمال نقص فنی ناشی از سوء استفاده عمدی یا تصادفی یا بروز نقص های طراحی است. ریسک به طور غیرمستقیم به دلیل اتکای یک شرکت به فناوری استقرار یافته افزایش می یابد. به سادگی، شرکت هایی که با موفقیت راه حل های فنی را به کار می گیرند، فناوری جدید را در تمام جنبه های معماری ادغام می کنند. بنابراین، اختلال ناگهانی یا در دسترس نبودن فناوری می تواند

اثرات نامطلوبی داشته باشد. ماهیت روندهای فنی اخیر خطرات منحصر به فردی را به همراه داشته است. این شامل مصرف گسترده فناوری اطلاعات از طریق دستگاه های تلفن همراه است. تحرک منجر به خطرات جدیدی شده است که می تواند به عنوان تهدیدی برای محرمانه بودن، یکپارچگی و در دسترس بودن، اساساً به دلیل ماهیت قابل حمل دستگاه های تلفن همراه و احتمال سرقت یا مفقود شدن دستگاه، تأثیر منفی بگذارد.

اگرچه مدیران کسب‌وکار صنعت مالی معمولاً از کشف یک رخنه تعجب می‌کنند، موفقیت نفوذهای سایبری به مدیران ریسک فناوری شوک وارد نمی‌کند. سازه های مدیریت ریسک، همانطور که امروزه به طور کلی توسط کسب و کار پذیرفته شده است، قرن هاست که کم و بیش به همان شکل وجود داشته است. با این حال، ریسک امنیت سایبری مشکلی را نشان می دهد که تنها در چند دهه گذشته با در نظر گرفتن معیارهای ریسک عملیاتی رایج مورد بررسی قرار گرفته است.

در سال ۱۹۹۶، تاریخچه مدیریت ریسک به شکل اسنادی در کتابی از پیتر برنشتاین به نام *در برابر خدایان، داستان قابل توجه ریسک*[1] شرح داده شد. [2]خطر امنیت سایبری در این کتاب ذکر نشده است، و هیچ یک از ابزارهایی که اکنون توسط مدیران ریسک امنیت سایبری استفاده می شود، وجود نداشت. برنشتاین از روش های تجزیه و تحلیل داده ها که اکنون برای تجزیه و تحلیل خطرات امنیت سایبری استفاده می شود آگاه بود و از آنها به عنوان "ژیمناستیک کامپیوتری" یاد می کرد. به نظر برنشتاین، اولین ریاضیدانانی که به شانس فکر کردند، به راحتی می‌توانستند مجموعه‌ای از دانش را تشکیل دهند که نظریه احتمال را تشکیل می‌دهد، اما ایده استفاده از ریاضیات برای مدیریت ریسک تنها زمانی پدیدار شد که مردم شروع به این باور کردند که تصمیم‌های خودشان می‌تواند مسیر مشیت یا سرنوشت را پیش‌بینی کند. بنابراین در حالی که بانک‌ها برای قرن‌ها از مدل‌های اعتباری مانند برآورد وثیقه و نرخ بازده تجاری استفاده می‌کردند، مدل‌های ریاضی واقعی مبتنی بر آمارهای تاریخی تا عصر روشنگری برای هدایت تصمیم‌های تجاری استفاده نمی‌شد و تا قرن هفدهم رویه ترکیب داده‌های تاریخی با آمار در صنعت بیمه رایج شد. حتی امروزه، واضح ترین نمونه های تصمیم گیری ریسک مالی در بیمه و به دنبال آن ریسک اعتباری یافت می شود. چه اعتبار به یک مصرف کننده، کسب و کار یا نهاد دولتی تعلق گیرد، برخی از مدیران مالی باید شانس بازپرداخت مانده بدهی را تخمین بزنند. در مورد ریسک اعتباری مصرف‌کننده، مصرف‌کنندگان با استفاده از ابعاد گسترده‌ای مورد ارزیابی قرار می‌گیرند که مهم‌ترین آنها با استفاده از امتیازات اعتباری است که شاخص‌های ریسک هستند. اگرچه امتیاز FICO پرکاربردترین معیار است، امتیازهای بی‌شماری دیگر بر اساس مدل‌هایی وجود دارد که شامل جمعیت‌شناسی مصرف‌کننده، درآمد، اعتبار فعلی، تجربه قبلی بدهکار، ورشکستگی، رأی دادگاه و محکومیت قضایی می‌شود. بسیاری از بانک ها از چنین امتیازهایی در مدلی

[1] - Against the Gods, The Remarkable Story of Risk

[2] - Rohmeyer 2019.

استفاده می‌کند که بر اساس آن معیاری از احتمال را ایجاد می‌کند که آیا وام گیرنده(گیرنده اعتبار) تعهدات اعتباری خود را ایفا می کند یا خیر. این مدل ها اساساً بر اساس رفتار گذشته مصرف کنندگان مشابه در موقعیت های جمعیتی و مالی مشابه ساخته می شوند.

نمونه دیگری از حوزه ای که مدیران مالی معمولاً با تصمیمات مبتنی بر ریسک روبرو هستند، ریسک بازار است. راه اندازی یک محصول مالی جدید یا حرکت به یک بازار مالی جدید می تواند مملو از عدم اطمینان باشد. مدیران اجرایی تحقیقاتی را انجام می دهند که در آن مشتریان بالقوه برای تعیین احتمال پرداخت هزینه برای محصول جدید مورد بررسی قرار می گیرند. استراتژی‌های تبلیغاتی برای تخمین احتمال دستیابی به افرادی که به محصولات مشابه علاقه نشان می‌دهند، یا در غیر این صورت احتمالاً مشتری در نظر گرفته می‌شوند، تجزیه و تحلیل می‌شوند. برای تخمین احتمال تولید سودآور محصول از تامین کنندگان درخواست می شود. با داشتن چنین احتمالاتی، مدیران احتمال موفقیت آمیز بودن عرضه محصول را تخمین می زنند و تصمیمات را بر اساس این شانس ها قرار می دهند. در تمام موارد موفقیت آمیز کاربرد نظریه احتمال در مدیریت ریسک، تعداد زیادی داده مناسب در طول زمان جمع آوری شده است که در آن الگوهای پایدار تکرار می شوند. توجه داشته باشید که تصمیم ریسک اعتباری بیشتر بر اساس تجزیه و تحلیل داده های تاریخی است و تصمیم گیری در مورد ریسک بازار بیشتر بر اساس تجزیه و تحلیل رفتار بالقوه آینده است. مدل‌های مبتنی بر ریسک امنیت سایبری که از مجموعه داده‌های انبوه برای پیش‌بینی آینده استفاده می‌کنند، هنوز معمولاً توسط صنعت استفاده نمی‌شوند. بدون مدل‌هایی که از داده‌های گذشته برای پیش‌بینی آینده استفاده می‌کنند، هیچ راهی برای توافق بر روی احتمال پایه یک رویداد معین وجود ندارد. همانطور که برنشتاین بیان می‌کند، «ابزارهای پیش‌بینی مبتنی بر روش‌های غیرخطی یا ژیمناستیک رایانه‌ای در معرض بسیاری از موانعی هستند که بر سر راه نظریه احتمالات مرسوم قرار دارند به واقع ماده خام مدل، داده‌های گذشته است.

پارامترهای تصمیم گیری ریسک اعتباری در طول دهه ها از آغاز عصر اطلاعات اصلاح شده است. اگرچه مدل‌های تصمیم‌گیری ریسک بازار به‌اندازه ریسک اعتباری استاندارد نیستند لیکن پارامترهایی که مدل‌های تصمیم‌گیری ریسک بازار را تشکیل می‌دهند نیز طی دهه‌ها تحقیق و اصلاح شده‌اند. با این حال، عناصر داده استفاده در پیش‌بینی رویدادهای امنیت سایبری، هنوز به گونه‌ای استاندارد نشده‌اند که امکان اجماع در مورد شاخص‌های ریسک امنیت سایبری را فراهم کند. علاوه بر این، به نظر نمی رسد که جوامع استانداردی[1] به دنبال راه هایی برای ساختار داده های امنیت سایبری باشند تا رویدادهای آینده با استفاده از داده ها پیش بینی شوند.

[1] - Standards Communities

وقوع رویدادهای گذشته اگرچه برخی فشارهای نظارتی بر صنعت مالی برای بررسی چنین رویکردی را ایجاد نموده است، لیکن در حال حاضر هیچ معادلی برای امتیاز اعتباری برای امنیت سایبری وجود ندارد. به این معنا که شیوه‌های استاندارد مدیریت ریسک در تخصیص قابل اعتماد احتمال یک حمله سایبری موفق به دو سیستم یا مشتری متفاوت، به همان شیوه‌ای که یک بانکدار می‌تواند احتمال بازپرداخت موفق وام مسکن را تعیین کند، کاربرد چندانی ندارد.

۳-۲. کمبود داده های تاریخی کافی

جان داودی از مکینزی مشاهده کرد که درک ضعیفی از تهدیدات سایبری به دلیل اطلاعات ناکافی در مورد حملات سایبری واقعی وجود دارد. یکی از دلایل فقدان داده‌ها عدم اشتراک‌گذاری اطلاعات سایبری دقیق از سوی کسانی است که پاسخ‌های تهدیدات سایبری را در دولت و بخش خصوصی مدیریت می‌کنند. به عبارت دیگر اگرچه متخصصان امنیت سایبری به طور کامل میزان تهدیدات را درک می کنند، اما عموم مردم شواهد مشخص و ملموس بسیار کمی از تهدیدات فوری را می بینند. علاوه بر این، فقدان اطلاعات تهدید منجر به دست کم گرفتن سیستماتیک ارزش دارایی های اطلاعاتی در معرض خطر می شود. لذا چالش اساسی اطلاعات ناکافی برای کسانی که به دنبال یادگیری در مورد ماهیت و بزرگی تهدیدات سایبری هستند، عدم اطمینان ایجاد می کند. در حالی که باید انتظار داشت کمبود اطلاعات برای مدتی در آینده به عنوان یک چالش باقی بماند، جزئیات قابل توجهی در حوزه عمومی وجود دارد که راهنمایی های مفیدی در مورد ماهیت حملات سایبری ارائه می دهد. بنابراین، در حالی که اطلاعات موجود تا حدودی ناقص است، سرنخ های مهمی برای پشتیبانی از درک ویژگی های مهم تهدید ارائه می دهد.

تازه واردان به حوزه امنیت سایبری ممکن است از تضاد فاحش بین منابع مختلفی که به طورهمه جانبه حملات امنیت سایبری را اعلام می کنند و داده های واقعی موجود برای مطالعه خطرات امنیت سایبری شگفت زده شوند. این وضعیت مطمئناً نتیجه عدم تلاش متخصصان امنیت سایبری برای جمع آوری و اشتراک گذاری داده ها نیست. در واقع، از اولین کنفرانس مؤسسه ملی استانداردها و فناوری (NIST) در مورد معیارهای امنیتی که تا کنون ایجاد شده، مرکز تجزیه و تحلیل سیستمی مالی و انعطاف پذیری (FSARC) ، تلاش‌های قهرمانانه‌ای برای جمع‌آوری داده‌های بیشتر و بهتر برای حمایت از تحلیل ریسک امنیت سایبری صورت گرفته است. برجسته‌ترین تلاش‌ها در این بین، گزارش نقض داده DB8 و Vocabulary for Event Recording and Incident Sharing (VERIS) بوده است. هر دو جزئیاتی در مورد حوادث امنیت سایبری ارائه کرده‌اند، اما با چالش جمع‌آوری سطحی از جزئیات لازم برای استفاده از منظر آماری دست و پنجه نرم کرده‌اند. گزارش VERIS که به عنوان گزارش تحقیقات نقض داده‌های Verizon (DBIR) نیز شناخته می‌شود، غنی‌ترین گزارش است و شامل اطلاعات موردی

از منابع متعدد از جمله تیم‌های واکنش عمومی و خصوصی، سازمان‌های بین‌المللی اجرای قانون، فروشندگان نرم‌افزار و خدمات امنیت سایبری و اتاق‌های فکر است. با این وجود، داده هایی که در اختیار داریم به اندازه کافی دارای جزئیات معنی دار به منظور پیش بینی نیستند. داده های مربوط به رخداد[1] معمولاً در طبقات مقایسه پذیر دسته بندی می شوند که در چارچوب زمانی تحلیل به وقوع پیوسته اند و قابل انتساب به سازمانی های هستند که دارای ویژگی های مشابه اند. با این حال، داده های مزبور نشان دهنده طیف قابل توجهی از حملات سایبری نیست. DataLoss DB با این انتظار که بتواند خدمات اشتراک داده ها را ارائه دهد عملاً ناموفق بود و منحل شد. همانطور که گزارش VERIS در جدیدترین انتشار خود اعتراف کرد، *"ما هیچ راهی برای دانستن اینکه چه نسبتی از رخنه در داده ها[2] قابل مشاهده است نداریم، زیرا هیچ راهی برای اطلاع از تعداد کل رخنه در داده ها در همه سازمان ها در سال ۲۰۱۶ در دسترس نیست. بسیاری از رخنه در داده ها گزارش نمی شوند (اگرچه نمونه ما حاوی بسیاری از آنهاست). بسیاری از موارد دیگر هنوز توسط قربانی ناشناخته هستند."*[3] علاوه بر این فقط در صورتیکه حمله به قدری گسترده باشد که هزاران دستگاه را به طور هم‌زمان مورد اصابت قرار دهد، مانند WannaCry، داده‌های حادثه به صورت انبوه به اشتراک گذاشته می‌شوند، در سایر موارد جزئیات دقیق و فنی کافی برای امکان مقایسه ارائه نمی شوند بدین ترتیب اطلاعات حملات عملاً یکسان هستند و به مثابه این است که دو حمله در واقع نمونه های تکراری از یک حمله هستند. متأسفانه، امنیت سایبری یک مشکل شر بر انگیز[4] است، که ریشه شر در ماهیت مسئله است که راه‌حل نهایی و صحیح برای آن وجود ندارد، بلکه صرفاً هدف بهبود موقعیتی است که برنامه‌ریز برای آن مسئولیت رسمی دارد. اصطلاح شر بر انگیز و یا شرور برای توصیف یک مسئله اولین بار توسط جامعه شناسانی گرفت که در جستجوی صفتی بودند که دیدگاه آنها را نسبت به مشکلاتی مانند بی خانمانی و سوء مصرف مواد بیان کند. «ناتوانی در حل کامل» ویژگی مشترک اندازه‌گیری امنیت سیستم‌ها با چالش‌های علوم اجتماعی مزبور و شر برانگیزی مسئله بسزایی دارد. بواقع این امر دستیابی به مفهومی از امنیت که به عنوان یک سیستم ملموس قابل درک و نیز اعتبارسنجی اندازه گیری آن بر اساس استانداردهای علمی را دشوار می سازد. همانطور که Dan Geer، یکی از اعضای مؤسس Securitymetrics.org می گوید: " به عنوان آماردان باید پرسید که آیا در مرحله آزمایش فرضیه هستیم یا هنوز در مرحله تولید فرضیه ایم. من می دانم که در مورد دوم قراردارم، به همین دلیل است که کم و بیش به دنبال داده هایی هستم که بتوانم بر روی آنها تجزیه و تحلیل اکتشافی[5] انجام دهم. افرادی که داده‌ها را در اختیار دارند می‌توانند آزمایش فرضیه انجام دهند، لیکن بنابر

---

[1] - Incidents
[2] - Data Breach
[3] - Rohmeyer 2019.79
[4] - Wicked
[5] - Exploratory analysis

چارچوب علمی پس از انجام آزمون فرض لازم است که نتایج آن را با تکیه بر روش تحقیق بکار رفته گزارش نمایند. محققین دیگر نیز می توانند بر اساس داده های خود صحت نتایج بدست آمده را بررسی نمایند".

هرچند بدون استفاده از داده و اندازه گیری احتمال نیز به تحلیل نفوذ پرداخت. با اطمینان مطلق از این که تمام سیستم های متصل به اینترنت به طور مداوم توسط نیروهای مخربی که از تکنیک های خودکار و دستی استفاده می کنند، اسکن می شوندبه احتمال زیاد آسیب‌پذیری‌ها در هر سیستم متصل به اینترنت پیدا شده و مورد سوء استفاده قرار می‌گیرند. ناشناخته این است که آیا یک دشمن خاص هر سیستمی را هدف قرار خواهد داد یا خیر. در طول دهه گذشته، برخی از داده ها در مورد اهداف جمع آوری شده است. این از سال به سال تغییر می کند، اما وابستگی به صنعت مالی معمولاً یک نقطه داده جمع آوری شده است. یکی از غنی‌ترین مطالعات درباره نقض‌های امنیتی، گزارش سالانه Verizon Data Breach Investigations Report (DBIR) است که شامل اطلاعات موردی از منابع متعدد از جمله تیم‌های واکنش عمومی و خصوصی، آژانس‌های بین‌المللی اجرای قانون، فروشندگان نرم‌افزار و خدمات امنیت سایبری و اتاق‌های فکر است. .

بر اساس DBIR، در سال ۲۰۱۶ ۲۴ درصد از نقض اطلاعات امنیت سایبری گزارش شده مربوط به صنعت مالی بوده است. مراقبت های بهداشتی با سهم ۱۵ درصد در رتبه دوم، دولت با ۱۲ درصد در رتبه سوم و باقیمانده ۴۹ درصد مربوط ۱۸ صنعت دیگر می باشد[1]. بر این اساس هرچند سهم صنعت مالی ۲۴ درصد بوده است لیکن تنها ۱ درصد از حوادث ثبت شده منجر به نقض واقعی داده ها شده است. بنابراین، اگرچه هر مؤسسه باید احتمال تهدید را بر اساس آگاهی موقعیتی خود تخمین بزند، بهترین داده‌های موجود نشان می‌دهد که برای هر حمله معینی شانس اینکه هدف یک مؤسسه مالی باشد حدود ۱ از ۴ است. برای روشن تر شدن موضوع، اغراق آمیز نیست که ادعا کنیم دشمنان همه سیستم های متصل به اینترنت را که در همه شرکت های خدمات مالی ثبت شده اند اسکن می کنند، و اینکه برای هر یک از مدیران خدمات مالی آشکارا سهل انگاری است که احتمال اینکه شرکت آنها برای هر نوع آسیب پذیری اعم از قدیمی یا جدید اسکن شود را کمتر از ۱۰۰ درصد در نظر گرفته شود. بر این اساس باید بطور شفاف گفت که دشمنان می توانند از هر سیستم آسیب پذیری سوء استفاده کنند و در نتیجه احتمال اینکه یک سیستم مالی آسیب پذیر مورد سوء استفاده قرار گیرد بر این اساس است که آیا یک شرکت هدف اسکن قرار گرفته است یا خیر تعیین نمی شود بلکه نکته کلیدی و مهم اینجاست که آیا دشمن که سیستم آسیب پذیر را در اسکن می یابد تصمیم می گیرد که از آسیب پذیری در تعقیب هدف سرقت اطلاعات به منظور تقلب یا اختلال سوء استفاده کند یا خیر. بدین ترتیب معیار ریسک بهره برداری مجرمانه از اطلاعات باید بر اساس جذابیت یک سیستم به عنوان یک هدف برای یک دشمن خاص باشد. بنابراین بر اساس مبانی علم

[1] - Rohmeyer 2019.80

احتمالات و آمار، احتمال آسیب ناشی از نفوذ را می توان از رابطه احتمال شرطی محاسبه نمود. بدین منظور اگر رویداد نفوذ را با A و سوء استفاده را با B نشان دهیم در این صورت رویداد آسیب ناشی از نفوذ عبارت خواهد بود از $A \cap B$. بر این اساس احتمال آسیب پذیری از روابط زیر بدست می آید:

$$P(A \cap B) = P(A)P(B|A)$$

حال اگر دو رویدار مستقل باشند داریم $P(B|A) = P(B)$ در نتیجه خواهیم داشت:

$$P(A \cap B) = P(A)P(B)$$

اگر این دو رویداد مستقل از یکدیگر باشند با فرض اینکه احتمال هریک کوچک تر از یک باشد احتمال آسیب ناشی از نفوذ کمتر از هر یک از دو احتمال نفوذ و سوء استفاده خواهد بود. برای مثال اگر احتمال آسیب پذیر بودن یک سیستم و احتمال سوء از آن به ترتیب ۷۵ درصد و ۷۵ درصد باشد، احتمال آسیب ناشی از نفوذ به ترتیب زیر محاسبه می شود:

$$P(A \cap B) = P(A)P(B) = 0.75 \times 0.75 = 0.5625$$

فرض استقلال به شکلی که مثال زده شد می تواند گمراه کننده باشد چرا که ممکن است علی رغم اینکه مدیراجرایی می داند که احتمال نفوذ بالاست لیکن احتمال آسیب دیدن را در حد یک شیر یا خط ساده تلقی نماید. در دنیای واقعی فرض اینکه احتمالات مورد نظر مستقل ازیک دیگر باشند چندان قابل قبول نیست زیرا عوامل مختلفی ازمحیطی و سیستمی این دو را به یکدیگر وابسته می کند و در حالت اکستریم احتمال شرطی مزبور می تواند ۱ باشد در این صورت احتمال محاسبه شده قبلی به ترتیب زیر خواهد بود :

$$P(A \cap B) = P(A)P(B|A) = 0.75 \times 1 = 0.75$$

۳. فصل سوم : مبانی محاسباتی مدیریت ریسک امنیت سایبری

۳-۱. مفهوم اندازه گیری[1]

"آنجا که گزاره های ریاضی به واقعیت اشاره دارند، یقینی نیستند؛ و جایی که یقین دارند به واقعیت رجوع نمی کنند." -آلبرت انیشتین

"اگرچه ممکن است این یک پارادوکس به نظر برسد، اما تمام علوم دقیق مبتنی بر ایده تقریب است. اگر فردی به شما بگوید که موضوعی را دقیقاً می داند، در این صورت می توانید با خیال راحت استنباط کنید که با فردی نادرست صحبت می کنید." – برتراند راسل (۱۹۷۰-۱۸۷۲)، ریاضی‌دان و فیلسوف بریتانیایی

در مورد افرادی که چیزی را غیرقابل اندازه‌گیری می‌دانند، مفهوم اندازه‌گیری – یا بهتر است بگوییم تصور نادرست از آن – احتمالاً مهم‌ترین مانعی است که باید بر آن غلبه کرد. اگر به اشتباه فکر کنیم که اندازه‌گیری به معنای دستیابی به برخی استانداردهای قطعیت تقریباً دست نیافتنی است، آنگاه چیزهای کمی حتی در علوم فیزیکی قابل اندازه‌گیری خواهند بود. اگر از یک مدیر یا کارشناس امنیت سایبری بپرسید اندازه‌گیری به چه معناست، معمولاً پاسخ‌هایی مانند «کمیت‌سازی چیزی»، «محاسبه یک مقدار دقیق»، «کاهش به یک عدد واحد» یا «انتخاب یک مقدار معرف» دریافت می‌کنید. آنچه به طور ضمنی یا صریح در همه این پاسخ ها این است که اندازه گیری یک عدد واحد و دقیق است که جایی برای خطا ندارد. اگر واقعاً معنای این اصطلاح همین بود، در واقع، موارد بسیار کمی قابل اندازه‌گیری بودند. شاید خواننده چیزی مانند این را شنیده یا گفته باشد: «ما نمی‌توانیم تأثیر واقعی نقض داده را اندازه‌گیری کنیم، زیرا برخی از عواقب آن را نمی‌توان دقیقاً شناخت». یا شاید، «به هیچ وجه نمی‌توانیم احتمال اینکه هدف یک حمله به منظور جلوگیری از دسترسی به خدمات[2] قرار بگیریم، را به دلیل عدم اطمینان بسیار بالا تعیین کنیم». این عبارات بیانگر یک تعریف فرضی از اندازه گیری که هم بی ارتباط با تصمیم گیری واقعی و هم غیرعلمی است. وقتی دانشمندان، آکچوئرها یا آماردانان اندازه گیری را انجام می دهند، از تعریف واقعی متفاوتی استفاده می کنند.

۳-۲. تعریف اندازه گیری

[1] - Hubbard and Seiersen 2016.,p.20-30

[2] - Denial-of-Service

برای تمام اهداف تصمیم گیری عملی، ما باید اندازه گیری را به عنوان مشاهداتی در نظر بگیریم که به طور کمی عدم قطعیت را کاهش می دهند. کاهش صرف، نه لزوماً حذف، عدم قطعیت برای اندازه گیری کافی است. حتی اگر برخی از دانشمندان این تعریف را دقیقاً بیان نکنند، روش‌هایی که استفاده می‌کنند روشن می‌کند که برای آنها اندازه‌گیری فقط یک تمرین احتمالی است. اطمینان در مورد کمیت های دنیای واقعی معمولاً از دسترس آنها خارج است. این واقعیت که مقداری از خطا اجتناب ناپذیر است، اما همچنان می تواند باعث بهبود دانش قبلی شود، در نحوه انجام آزمایش ها، بررسی ها و سایر اندازه گیری های علمی نقش اساسی دارد.بدین ترتیب می توان اندازه‌گیری را کاهش عدم قطعیت به صورت کمی بر اساس یک یا مشاهده تعریف نمود. تفاوت های عملی بین این تعریف و محبوب ترین تعاریف اندازه گیری بسیار زیاد است. یک اندازه‌گیری واقعی نه تنها نیازی به دقت بی‌نهایت ندارد تا به عنوان اندازه‌گیری در نظر گرفته شود، بلکه عدم وجود خطای گزارش شده - که به معنای دقیق بودن عدد است - می‌تواند نشانه‌ای از عدم استفاده از روش‌های تجربی، مانند نمونه‌گیری و آزمایش‌ها باشد (یعنی، این واقعاً یک اندازه گیری نیست). اندازه‌گیری‌هایی که استانداردهای اولیه اعتبار علمی را تأمین می‌کنند، نتایج را با درجه مشخصی از عدم قطعیت گزارش می‌کنند، مانند: «به احتمال ۹۰ درصد حمله به این سیستم باعث از کار افتادن آن بین ۱ تا ۸ ساعت می‌شود». این تصور از اندازه‌گیری ممکن است جدید باشد، اما پایه‌های ریاضی قوی - و همچنین دلایل عملی - برای نگاه کردن به اندازه‌گیری از این طریق وجود دارد. اندازه گیری در نهایت فقط اطلاعات است و ساختار نظری دقیقی برای اطلاعات وجود دارد. رشته ای به نام "نظریه اطلاعات" در دهه ۱۹۴۰ توسط کلود شانون[1]، مهندس برق و ریاضیدان آمریکایی توسعه یافت. در سال ۱۹۴۸، او مقاله‌ای با عنوان «نظریه ریاضی ارتباطات» منتشر کرد که پایه و اساس نظریه اطلاعات و در نهایت بسیاری از دنیای فناوری اطلاعات را که متخصصان امنیت سایبری در آن کار می‌کنند، بنا نهاد.

۳-۳. طبقه بندی مقیاس های اندازه گیری

بر اساس آنچه گفته شد اندازه گیری امنیت سایبری مانند هر اندازه گیری دیگری است و نیازی به اطمینان ندارد. انواع مختلف مقیاس‌های اندازه‌گیری می‌توانند درک ما از اندازه‌گیری را بیش‌تر پیش ببرند. معمولاً، ما تصور می‌کنیم که اندازه‌گیری‌ها شامل یک واحد اندازه‌گیری مشخص و کاملاً تعریف‌شده مانند دلار در سال در بودجه امنیت سایبری یا دقیقه‌های مدت زمان توقف سیستم است. اما آیا مقیاسی مانند "بالا"، "متوسط" یا "کم" می تواند یک مقیاس مناسب را تشکیل دهد. متخصصان امنیت سایبری مقیاس هایی از این دست را در بسیاری از

[1] - Claude Shannon

استانداردها و شیوه ها در همه زمینه های ارزیابی ریسک در نظر می گیرند. معمولاً مشاهده می شود که مقادیری مانند «تاثیر» یا «احتمال» به صورت ذهنی در مقیاس ۱ تا ۵ ارزیابی می شوند و سپس این مقیاس ها برای ارزیابی ریسک به عنوان بالا، متوسط یا پایین بیشتر ترکیب می شوند. اینها روشهای فریبنده ساده ای هستند که مجموعه ای از مسائل را معرفی می کنند که در ادامه سعی می کنیم با جزئیات بیشتر مورد بحث قرار در هیم. اما مواردی را در نظر بگیرید که ممکن است استفاده از مقیاس های غیر از واحدهای اندازه گیری معمولی منطقی باشد. توجه داشته باشید بنابر تعریفی که در اینجا ارائه می شود لازم است اندازه‌گیری «به صورت کمی بیان می‌شود». بنابر این عدم قطعیت، حداقل، باید کمی شود، اما موضوع مشاهده ممکن است یک کمیت نبوده و کاملاً کیفی باشد، مانند عضویت در یک مجموعه. به عنوان مثال، ما می‌توانیم چیزی را «اندازه‌گیری» کنیم که در آن پاسخ بله یا خیر است برای مثال آیا نقض داده‌ها در سال جاری اتفاق می‌افتد یا ادعای بیمه سایبری مطرح می‌شود در حالی که هنوز تعریف دقیق خود را از اندازه‌گیری برآورده می‌کنیم. اما عدم قطعیت ما در مورد آن مشاهدات هنوز باید به صورت کمی بیان شود (به عنوان مثال، ۱۵٪ احتمال نقض داده در سال جاری وجود دارد، احتمال ۲۰٪ برای ادعای بیمه سایبری وجود دارد). این دیدگاه که اندازه گیری در مورد سوالات با پاسخ بله/خیر اعمال می شود یا سایر تمایزات کیفی با مکتب فکری پذیرفته شده دیگری در مورد اندازه گیری سازگار است. در سال ۱۹۴۶ روانشناسی به نام استنلی اسمیت استیونز[1] مقاله ای با عنوان « نظریه مقیاس ها و اندازه گیری» نوشت. او در آن مقاله چهار مقیاس مختلف اندازه گیری را توصیف می کند: مقیاس اسمی، ترتیبی، فاصله ای و نسبی. اگر خواننده به درجه سانتیگراد یا دلار به عنوان اندازه گیری فکر می کند، به ترتیب به مقیاس فاصله و نسبت می اندیشد. این ترازوها هر دو دارای یک "واحد" کاملاً مشخص با اندازه منظم هستند. در هر دو مورد می توانیم بگوییم ۲۶ بیشتر از ۴ است (۶ درجه سانتیگراد یا ۶ دلار). با این حال، یک مقیاس فاصله‌ای واقعاً به ما اجازه نمی‌دهد بگوییم که ۶ «۵۰ درصد بیشتر» از ۴ یا «دو برابر بیشتر» از ۳ است. برای مثال، ۶ درجه سانتی‌گراد «دو برابر گرمتر» از ۳ درجه سانتیگراد نیست. (از آنجایی که موقعیت "صفر" در مقیاس سانتیگراد به طور دلخواه در نقطه انجماد آب تنظیم شده است). اما ۶ میلیون دلار دو برابر ۳ میلیون دلار است. بنابراین، برخی از عملیات های ریاضی مانند ضرب یا تقسیم وجود دارد که نمی توانیم در مقیاس های فاصله از آنها استفاده نماییم. مقیاس های اسمی و ترتیبی حتی محدودتر هستند. یک مقیاس اسمی هیچ ترتیب یا بزرگی ضمنی ندارد مانند جنسیت یا مکان یا اینکه آیا یک سیستم ویژگی خاصی دارد یا خیر. مقیاس اسمی حالتی را بیان می کند بدون اینکه بگوید یک حالت دو برابر حالت دیگر است یا حتی، در این مورد، بیشتر یا کمتر از دیگری است – هر مقیاس حالت فقط یک حالت متفاوت است، نه یک حالت بالاتر یا پایین تر. از سوی دیگر مقیاس های ترتیبی یک ترتیب را نشان می دهند اما

[1] - Stanley Smith Stevens

نه بر میزان آن. مثلاً می‌توانیم بگوییم که شخصی با حقوق مدیریت دارای امتیازات بیشتری نسبت به یک کاربر معمولی است. لیکن نمی توانیم بگوییم که این امتیاز پنج برابر یک کاربر معمولی و یا دو برابر بیشتر از یک کاربر دیگر است. بنابراین اکثر عملیات های ریاضی به غیر از منطق پایه یا عملیات مجموعه برای مقیاس های اسمی یا ترتیبی قابل اجرا نیستند. با این حال هرچند مقیاس های اسمی و ترتیبی با مقیاس های اندازه گیری معمولی مانند کیلوگرم و ثانیه متفاوت هستند این امکان وجود دارد که اطلاعات آموزنده ای را از آنها بدست آورد. برای یک زمین شناس، مفید است که بداند یک سنگ از سنگ دیگر سخت تر است، بدون اینکه لزوماً بداند چقدر است. روشی که آنها برای مقایسه سختی کانی ها استفاده می کنند مقیاس سختی Mohs نام دارد که یک مقیاس ترتیبی است. بنابراین، استفاده از مقیاس‌های ترتیبی مانند مقیاس‌هایی که اغلب در امنیت سایبری یافت می‌شوند، به‌طور جدی نقض مفاهیم اندازه‌گیری نیست، اما نحوه انجام آن، آنچه که در مورد آن اعمال می‌شود، و آنچه بعد از آن با این مقادیر انجام می‌شود، می تواند اصول اولیه را نقض کرده و می‌تواند باعث بسیاری از مشکلات شود. به طور مثال زمین شناسان مقادیر مقیاس سختی Mohs را در رنگ سنگ ضرب نمی کنند. هرچند مقیاس Mohs یک اندازه گیری کاملاً تعریف شده است، استفاده از مقیاس های ترتیبی در امنیت سایبری اغلب چنین نیست. در ادامه نشان خواهیم داد که معیارهای مبتنی بر مقادیر کاملاً تعریف شده – مانند احتمال سالانه یک رویداد و توزیع احتمال ضررهای احتمالی به انواع مقیاس های ترتیبی که معمولاً در امنیت سایبری استفاده می شود ارجحیت دارند. در واقع، هیچ چیز در علم و مهندسی واقعاً به مقیاس ترتیبی متکی نیست. حتی مقیاس سختی Mohs در بسیاری از مصارف جایگزین شده است. (در خارج از زمین شناسی، مقیاس ویکرز[1]، یک مقیاس نسبت مناسب، برای مواد در مسائل علوم و مهندسی مناسب تر در نظر گرفته می شود.) همه اینها تمایزات مهمی در مورد مفهوم اندازه گیری هستند که شامل درس های زیادی برای مدیران به طور کلی و همچنین متخصصان امنیت سایبری است. این تصور رایج که اندازه گیری ها را کمیت های دقیق فرض می کند، سودمندی صرفاً کاهش عدم قطعیت را در صورتی که حذف عدم قطعیت ممکن یا مقرون به صرفه نباشد نادیده می گیرد.حتی لازم نیست همه اندازه گیری ها در مورد یک کمیت معمولی باشند. اندازه‌گیری برای نقاط مورد علاقه اسمی و گسسته اعمال می‌شود، مانند «آیا با نفوذ عمده در داده ها مواجه خواهیم شد یا خیر؟» و همچنین مقادیر مستمری مانند "اگر نفوذ به داده مواجه شدیم چقدر هزینه خواهد داشت؟" شایان ذکر است که در فعالیت های تجاری، تصمیم گیرندگان در شرایط عدم قطعیت تصمیم می گیرند. وقتی این عدم اطمینان در مورد تصمیمات بزرگ و پرخطر باشد، کاهش عدم قطعیت ارزش زیادی دارد و به همین دلیل است که ما از این تعریف اندازه گیری استفاده می نماییم.

[1] - Vickers Scale

۴-۳. اندازه گیری بیزی: یک مفهوم عملی برای تصمیم گیری

"بنابراین منطق صحیح برای این جهان حسابان احتمالات[1] است،که بر اساس آن بزرگی احتمالی را در نظر می گیرد که بر اساس ذهن یک انسان منطقی وجود دارد یا باید باشد." جیمز کلرک ماکسول[2]، ۱۸۵۰

وقتی از اندازه‌گیری به عنوان «کاهش عدم قطعیت» صحبت می‌کنیم، به این معنا اشاره می‌کنیم که یک وضعیت قبلی عدم قطعیت وجود دارد که باید کاهش یابد و از آنجایی که این عدم قطعیت می تواند در نتیجه مشاهدات تغییر کند، ما عدم قطعیت را به عنوان ویژگی مشاهده گر در نظر می گیریم، نه لزوماً چیزی که مشاهده می شود. وقتی تست نفوذ را روی یک سیستم انجام می دهیم، با این بازرسی وضعیت برنامه را تغییر نمی دهیم. در عوض، ما در حال تغییر عدم اطمینان خود در مورد وضعیت برنامه هستیم. ما کمی نمودن عدم قطعیت اولیه و تغییر در عدم قطعیت را از مشاهدات و با استفاده از احتمالات انجام می دهیم. این بدان معنی است که ما از اصطلاح "احتمال" برای اشاره به وضعیت عدم اطمینان یک ناظر یا آنچه برخی "درجه اعتقاد"[3] نامیده اند استفاده می کنیم. اگر تقریباً مطمئن هستید که یک سیستم معین مورد نفوذ قرار می گیرد، می توانید بگویید که با احتمال ۹۹٪ این امر اتفاق می افتد. اگر مطمئن نیستید، ممکن است بگویید ۵۰ درصد احتمال وجود دارد. اختصاص دادن این احتمالات به صورت ذهنی در واقع مهارتی است که می توان یاد گرفت . به همین ترتیب، اگر در مورد مدت زمان خارج شدن یک سرویس از دسترس بسیار نامطمئن هستید، ممکن است بگویید به احتمال ۹۰ درصد مقدار واقعی بین ۱۰ دقیقه تا ۲ ساعت کاهش می یابد. اگر اطلاعات بیشتری داشتید، ممکن است دامنه بسیار باریک تری بدهید و همچنان یک احتمال ۹۰ درصدی را تعیین کنید که مقدار واقعی در آن محدوده قرار می گیرد.

این دیدگاه احتمالات را «سوبژکتیویستی» [4] یا ذهنی و یا گاهی اوقات تفسیر «بیزی» احتمالات می نامند[5]. الهام‌بخش اصلی تفسیر بیزی، توماس بیز، ریاضی‌دان و وزیر پروتستان بریتانیایی قرن هجدهم بود که مشهورترین سهمش در آمار تا پس از مرگش منتشر نشد. فرمول ساده او که به عنوان قضیه بیز شناخته می شود، توضیح می دهد که چگونه اطلاعات جدید می توانند احتمالات قبلی را به روز کنند. احتمال «پیشین»[6] می‌تواند به وضعیت عدم قطعیت اشاره کند که عمدتاً توسط داده‌های ثبت‌شده قبلی اطلاع‌رسانی می‌شود، اما همچنین می‌تواند به نقطه‌ای قبل از هر مشاهدات عینی و ثبت‌شده اشاره کند. معمولاً به طور حداقلی احتمال پیشین اغلب به صورت ذهنی در نظر گرفته می شود. برای تصمیم گیری، این مرتبط ترین استفاده از کلمه "احتمال" است. این فقط چیزی

---

[1] - Calculus of Probabilities
[2] - James Clerk Maxwell
[3]- Degree of Belief
[4] - Subjectivist
[5] - Bayesian Interpretation
[6] - Prior

نیست که باید بر اساس داده های دیگر محاسبه شود. یک شخص با بیان یک احتمال، عدم قطعیت را نشان می دهد. توانایی بیان وضعیت عدم قطعیت قبلی نقطه شروع مهمی در تمام تصمیمات عملی است. در واقع، شما معمولاً از قبل یک عدم اطمینان قبلی دارید - حتی اگر ممکن است به صراحت احتمالات را بیان نکنید. بیان پیشین‌ها حتی به ما امکان می‌دهد ارزش اطلاعات اضافی را محاسبه کنیم، زیرا، البته، ارزش اطلاعات اضافی حداقل تا حدی به وضعیت فعلی عدم اطمینان شما قبل از جمع‌آوری اطلاعات بستگی دارد. رویکرد بیزی این کار را انجام می دهد در حالی که برخی از مشکلات را تا حد زیادی ساده می کند و به ما امکان می دهد از اطلاعات محدود بیشتر استفاده کنیم. این تمایزی است که متخصصان امنیت سایبری باید آن را درک کنند. کسانی که احتمالات را فقط نتیجه محاسبات روی داده‌ها می‌دانند و نه بازتاب عدم قطعیت شخصی ، خواه بدانند یا ندانند، عملاً تفسیر خاصی از احتمال را فرض می‌کنند. آنها تفسیر «تکرارگرایی»[1] را انتخاب می‌کنند، و در حالی که ممکن است این را «عینی»[2] و علمی بدانند، بسیاری از آماردانان، ریاضی‌دانان و دانشمندان بزرگ می‌خواهند نگرش متفاوتی داشته باشند. (کتاب "چگونه هرچیزی را محاسبه کنیم" نوشته داگلاس هوبارد[3] "How to Measure Anything" توضیحی عمیقی از این تفاوت‌ها دارد.) بنابراین، اینکه فردی در امنیت سایبری بگوید که فاقد داده‌ها برای تعیین احتمالات است، اساساً یک طنز تلقی می شود چرا که ما از احتمال استفاده می کنیم زیرا اطلاعات کاملی نداریم. این موقعیت توسط پدر شناخته شده حوزه تحلیل تصمیم، پروفسور ران هاوارد[4] از دانشگاه استنفورد به بهترین وجه بیان شده است. در طی یک پادکست برای مصاحبه با هاروارد بیزینس ریویو[5]، مصاحبه کننده از هاوارد پرسید که چگونه با چالش تجزیه و تحلیل "وقتی احتمالات را نمی دانید" کنار می آیید. هاوارد پاسخ داد: خوب، ببینید، اما کل ایده احتمال این است که بتوانید با استفاده از اعداد میزان جهل و نادانی یا به طور معادل دانش خود را توصیف کنید. بنابراین مهم نیست که چقدر آگاه یا نادان باشید، این تعیین می کند که چه احتمالاتی با آن سازگار است. "ران هاوارد، پادکست بازنگری هاروارد،مصاحبه با جاستین فاکس، ۲۰ نوامبر ۲۰۱۴".

مواردی وجود دارد که "احتمال" یک مقدار محاسبه شده است، اما همانطور که ذهن های بزرگی مانند هاوارد و جیمز کلرک ماکسول بیان می کنند، از احتمال نیز برای نشان دادن وضعیت فعلی عدم اطمینان ما در مورد یک پدیده استفاده می شود، صرف نظر از اینکه این عدم قطعیت چقدر است. اما به خاطر داشته باشید که اگرچه این موضوع ذهنی است، اما احتمالی که به آن اشاره می کنیم فقط غیرمنطقی و دمدمی مزاج نیست. ما به عدم قطعیت های ذهنی نیاز داریم تا حداقل از نظر ریاضی منسجم و همچنین با مشاهدات مکرر و بعدی سازگار باشند. یک

---

[1] - Frequentist
[2] - Objective
[3] - Hubbard 2014.
[4] - Professor Ron Howard
[5] - Harvard Business Review

فرد منطقی نمی تواند به سادگی بگوید که به عنوان مثال، ۲۵ درصد احتمال دارد که سازمانش مورد حمله سایبری خاصی قرار گیرد و ۹۰ درصد احتمال دارد که چنین نشود (البته جمع این دو احتمال باید ۱۰۰٪ باشد). همچنین اگر کسی مدام می گوید که آنها ۱۰۰٪ از پیش بینی های خود مطمئن است ولی به طور مداوم این پیش بینی ها اشتباه هستند می توانیم عدم قطعیت های ذهنی وی را بر اساس دلایل عینی رد کنیم. درست همانطور که با خواندن یک ترازوی دیجیتال یا آمپرمتر شکسته انجام می دهیم. در نهایت، باید به یاد داشته باشیم که یک لبه دیگر برای شمشیر« کاهش عدم قطعیت» وجود دارد. حذف کامل عدم قطعیت برای اندازه گیری ضروری نیست اما باید مقداری کاهش عدم قطعیت وجود داشته باشد. تصمیم گیرنده یا تحلیلگر درگیر چیزی می شود که معتقد است فعالیت اندازه گیری است لیکن برآوردها و تصمیمات آن‌ها نه تنها حداقل بهبود نمی یابند بلکه بدتر می‌شوند، باید براساس تعریف بیان شده در خصوص اندازه گیری چنین استنباط نماییم که در واقع سپس آنها خطای خود را کاهش نداده اند. بنابراین، برای تعیین اینکه آیا این مقیاس های ترتیبی که در امنیت سایبری بسیار مورد استفاده قرار می گیرند معیارهای مناسبی هستند ، باید بپرسیم که آیا چنین مقیاس‌هایی واقعاً باعث کاهش عدم قطعیت می‌شوند یا خیر.

۵-۳. هدف اندازه گیری

"مشکلی که به خوبی بیان شود، مشکلی نیمه حل شده است."

چارلز کترینگ[1] (۱۸۷۶–۱۹۵۸)، مخترع آمریکایی، دارنده بیش از ۱۰۰ حق ثبت اختراع، از جمله سیستم جرقه زن الکتریکی برای اتومبیل

گفته فوق بسیار شبیه این عبارت است که ۵۰ درصد حل مسئله تعریف صحیح صورت مسئله است.

"هیچ مانعی برای پیشرفت دانش بیشتر از ابهام کلمات نیست."

- توماس رید[2](۱۷۹۶–۱۷۱۰)، فیلسوف اسکاتلندی

حتی زمانی که مفهوم مفیدتر اندازه گیری (به عنوان مشاهدات کاهش دهنده عدم قطعیت) پذیرفته می شود، برخی چیزها غیرقابل اندازه گیری به نظر می رسند زیرا ما به سادگی نمی دانیم که در اولین طرح سوال چه می گوییم. در این مورد، ما موضوع اندازه گیری را به طور واضح تعریف نکرده ایم. اگر کسی بپرسد که چگونه می توان "آسیب به شهرت" یا "تهدید" یا اختلال در کسب و کار را اندازه گیری کرد، ما به سادگی می پرسیم، "منظور شما دقیقاً چیست؟" جالب است که مردم چند وقت یکبار استفاده خود از این اصطلاح را به گونه ای اصلاح می کنند که تقریباً به خودی خود به سؤال اندازه گیری پاسخ می دهد. زمانی که مدیران متوجه منظورشان و دلیل

[1] - Charles Kettering
[2] - Thomas Reid

اهمیت آن شوند، موضوع مورد نظر بسیار قابل اندازه‌گیری‌تر به نظر می‌رسد. این معمولاً اولین سطح تجزیه و تحلیل است و زمانی که آقای داگلاس هابارد[1](نویسنده دو مرجع اصلی این نوشتار)، آنچه را «کارگاه‌های شفاف‌سازی» می‌نامد، برگزار می‌کند مطرح می نماید. موضوع صرفاً این است که مشتریان یک مورد خاص، اما در ابتدا مبهم را که می‌خواهند اندازه‌گیری کنند، بیان می‌کنند. برای این منظور فقط سوالاتی مانند "منظور شما از [در جای خالی] چیست" بپرسید؟ و "چرا برایت مهم است؟" این در مورد طیف گسترده ای از مشکلات اندازه گیری صدق می کند و امنیت سایبری نیز از این قاعده مستثنی نیست. در سال ۲۰۰۰، هنگامی که وزارت امور کهنه سربازان(افرادی که در خدمت سربازی برای کشورشان جنگیده اند)[2] از هابارد خواسته شد تا به تعریف معیارهای عملکرد جدید برای آنچه که "امنیت فناوری اطلاعات" نامیده می شود کمک کند، هابارد پرسید: "منظور شما از "امنیت فناوری اطلاعات" چیست؟ و طی دو سه کارگاه، کارکنان بخش برای او تعریف کردند و در نهایت معلوم شد که منظور آنها از امنیت فناوری اطلاعات چیزهایی مانند کاهش نفوذ و آلودگی های ویروسی بوده است. آنها توضیح دادند که این موارد از طریق کلاهبرداری، از دست دادن بهره وری یا حتی مسئولیت های قانونی بالقوه بر سازمان تأثیر می گذارد از جمله با بازیابی یک رایانه نوت بوک دزدیده شده در سال ۲۰۰۶ که شامل شماره های بیمه اجتماعی ۲۶/۵ میلیون کهنه سرباز بود، به سختی از اثرات منفی آن جلوگیری کردند. تقریباً در همه موارد، تأثیرات شناسایی شده به وضوح قابل اندازه گیری بودند. در این بین "امنیت" در ابتدای امر مفهومی مبهم بود و زمانی این ابهام رفع شد که آنها آن را به آنچه که واقعاً انتظار مشاهده داشتند تجزیه کردند. چیزی که ما آن را «زنجیره روشن‌سازی» می‌نامیم، فقط مجموعه‌ای کوتاه از روابط است که باید ما را از چیزی که آنرا ناملموس[3] تلقی می نماییم به سمت ملموس بودن[4] آن رهنمون نماید. اول، ما تشخیص می دهیم که اگر X چیزی است که ما به آن اهمیت می دهیم، پس X، طبق تعریف، باید به نحوی قابل تشخیص باشد. چگونه می‌توانیم به چیزهایی مانند «کیفیت»، «خطر»، «امنیت» یا «تصویر عمومی» اهمیت بدهیم، اگر این چیزها به هیچ وجه، مستقیم یا غیرمستقیم کاملاً غیرقابل شناسایی هستند؟ اگر دلیلی برای اهمیت دادن به مقداری ناشناخته داریم، به این دلیل است که فکر می کنیم به نحوی با نتایج مطلوب یا نامطلوب مطابقت دارد. ثانیاً، اگر این چیز قابل تشخیص است، پس باید تا حدودی قابل تشخیص باشد. اگر بتوانیم چیزی را مشاهده کنیم، می توانیم بخشی از آن را مشاهده نماییم. زمانی که این مقدار را بپذیریم، گام نهایی شاید ساده ترین قسمت مسئله باشد زیرا اگر بتوانیم مقداری آن را مشاهده کنیم، پس باید قابل اندازه گیری باشد.

با توجه به آنچه گفته شود زنجیره دسته بندی مسئله را می توان به ترتیب زیر تعریف نمود.

---

[1] - Douglas Hubbard
[2] - Veterans
[3] - Intangible
[4] - Tangible

- زنجیره شفاف سازی[1]

۱. اگر موضوعی مهم باشد، قابل تشخیص یا مشاهده است.

۲. اگر قابل تشخیص باشد، می توان آن را به صورت مقدار (یا محدوده ای ازمقادیر ممکن) در نظر گرفت.

۳. اگر بتوان آن را به عنوان طیفی از مقادیر ممکن تشخیص داد، حتماً قابل اندازه گیری است.

اگر زنجیره شفاف سازی کار نمی کند، ممکن است آنچه دانشمندان انجام می دهند و "آزمایش فکری" [2] نامیده می شود را امتحان کنید. برای این منظور تصور کنید شما یک دانشمند فرازمینی[3] هستید که می توانید نه تنها گوسفند یا حتی مردم بلکه کل سازمان ها را شبیه سازی کنید. شما یک جفت از همان سازمان را ایجاد می یکی را گروه "آزمون" و یکی را گروه "کنترل" می نامید. حال تصور کنید که در حالی که مقدار آن را در گروه کنترل ثابت نگه دارید، کمی بیشتر به گروه آزمایش «آسیب به شهرت» وارد کنید. تصور کنید واقعاً چه چیزی را به هر شکلی اعم از مستقیم یا غیرمستقیم مشاهده خواهید کرد که برای اولین سازمان تغییر می‌کند؟ آیا این به معنای کاهش فروش در کوتاه مدت یا بلند مدت است؟ آیا این بدان معناست که جذب متقاضیانی که می خواهند در شرکت های معتبر کار کنند سخت تر می شود؟ آیا به این معنی است که برای جبران این عواقب باید در کمپین های روابط عمومی پرهزینه شرکت کنید؟ اگر بتوانید حتی یک مشاهده را که بین دو سازمان شبیه سازی شده متفاوت است شناسایی کنید، در این صورت در راه شناسایی نحوه اندازه گیری آن هستید. همچنین به بیان اینکه چرا می‌خواهیم چیزی را اندازه‌گیری کنیم، کمک می‌کند تا بفهمیم چه چیزی واقعاً اندازه‌گیری می‌شود. هدف از اندازه گیری اغلب کلید تعیین این است که اندازه گیری واقعاً چه چیزی قرار است باشد. اندازه‌گیری‌ها باید همیشه از نوعی تصمیم حمایت کنند، چه آن تصمیم یکباره باشد یا یک تصمیم مکرر و مکرر. در مورد اندازه‌گیری ریسک‌های امنیت سایبری، احتمالاً در حال انجام اندازه‌گیری‌هایی برای تخصیص بهتر منابع برای کاهش خطرات هستیم. هدف از اندازه گیری سرنخ هایی در مورد معنای واقعی اندازه گیری و نحوه اندازه گیری آن به دست می دهد. علاوه بر این، چندین مورد بالقوه دیگر را پیدا کردیم که ممکن است برای حمایت از تصمیم مربوطه نیاز به اندازه‌گیری داشته باشند. شناسایی موضوع اندازه گیری واقعاً آغاز تقریباً هر تحقیق علمی از جمله تحقیقات واقعاً انقلابی است. کارشناسان و مدیران امنیت سایبری باید بدانند که برخی چیزها تنها به این دلیل نامشهود به نظر می‌رسند که تعریف ضعیفی از آنها ارائه شده است. عبارات مبهم مانند "قابلیت تهدید" یا "آسیب به شهرت" یا "اعتماد به مشتری" در ابتدا غیرقابل اندازه گیری به نظر می رسد، شاید فقط به این دلیل که منظور آنها به خوبی درک نشده است. این اصطلاحات ممکن است در واقع فهرستی از پدیده های متمایز و قابل

---

[1] - Clarification Chain
[2] - Thought Experiment
[3] - Alien Scientist

مشاهده را نشان دهند که برای فهمیدن نیاز به شناسایی دارند. بر این اساس در ادامه در حد ممکن راههایی را برای تجزیه آنها ارائه می شود. لیکن همانطوری که اشاره شد ابتدا لازم است د با تعریف برخی از اصطلاحات دیگر که تاکنون بارها استفاده کرده ایم، هدف اندازه گیری را روشن کنیم. برای اندازه گیری امنیت سایبری، ابتدا باید سؤالاتی مانند منظور ما از امنیت سایبری چیست یا چه تصمیماتی به اندازه گیری آن بستگی دارد، بپرسیم. برای بیشتر مردم، افزایش امنیت در نهایت باید به معنای چیزی بیش از این باشد که مثلاً چه کسی در آموزش های امنیتی شرکت کرده است یا چه تعداد از رایانه های رومیزی که نرم افزار امنیتی جدید نصب کرده اند. اگر امنیت بهتر است، برخی از خطرات باید کاهش یابد. اگر چنین است، پس باید بدانیم که منظورمان از ریسک چیست. روشن شدن این مشکل مستلزم آن است که به طور مشترک عدم اطمینان و ریسک را روشن کنیم. آنها نه تنها قابل اندازه گیری هستند بلکه کلید درک اندازه گیری به طور کلی هستند. بنابراین بیایید این اصطلاحات و معنای اندازه گیری آنها را تعریف کنیم.

۶-۳. تعاریف عدم قطعیت و ریسک و اندازه گیری آنها

- عدم قطعیت:

شرایطی که قطعیت کامل وجود ندارد بدین معنی که حالت های متعددی برای وقوع ممکن است و پیامد، وضعیت، همچنین نتیجه و ارزش به طور واقعی مشخص نیست.

- اندازه گیری عدم قطعیت:

فرآیندی که مجموعه ای از احتمالات که به مجموعه ای از اتفاقات اختصاص داده می شود. به عنوان مثال: "به احتمال ۲۰٪ ما در پنج سال آینده با نقض اطلاعات روبرو خواهیم شد."

- ریسک: حالتی از عدم قطعیت که در آن احتمال وقوع ضرر، فاجعه یا سایر پیامدهای نامطلوب وجود دارد.
- اندازه‌گیری ریسک: مجموعه‌ای از احتمالات، که هر کدام دارای احتمالات و زیان‌های کمی هستند. به عنوان مثال: "ما معتقدیم که احتمال ۱۰٪ وجود دارد که نقض داده ها منجر به مسئولیت قانونی بیش از ۱۰ میلیون دلار شود."

۴. فصل چهارم : مدل کاربردی کمی سازی امنیت سایبری[1]

کمی بساز، کمی آزمایش کن، چیزهای زیادی یاد بگیر.

دریاسالار دوم وین مایر، مدیر برنامه سیستم سلاح Aegis[2]

در این بخش یک نقطه شروع ساده برای توسعه یک ارزیابی کمی ریسک ارائه می شود که می توان بر اساس آن مدل‌های دقیق‌تر و روش‌های پیشرفته‌تری بنا نهاد. اما در حال حاضر با مدلی شروع خواهیم کرد که صرفاً جایگزین ماتریس ریسک رایج می شود. این به سادگی راهی برای گرفتن تخمین های ذهنی از احتمال و تأثیر خواهد بود، اما این کار را به صورت احتمالی انجام دهید. برای اینکه بتوانیم این کار را انجام دهیم، باید چند روش را معرفی کنیم. ابتدا، لیکن ابتدا لازم است که ایده ارزیابی ذهنی احتمالات را معرفی کنیم، همچنین یک روش شبیه سازی بسیار ابتدایی را معرفی خواهیم کرد و کار ساخت واقعی شبیه سازی بیشتر برای شما انجام می شود. مثال ها با استفاده از صفحات اکسل انجام داده شده است که امکان دانلود آن از آدرس اینترنتی www.howtomeasureanything.com/cybersecurity وجود دارد. پس از پایان این قسمت پایه و اساس لازم برای ایجاد روش های بهبود یافته فراهم می شود و در قسمت های بعد به تدریج این روش را می توانیم توسعه دهیم. بدین ترتیب یاد خواهید گرفت که چگونه ارزیابی های ذهنی خود را از احتمال آزمایش کنید و آنها را بهبود بخشید. بر این اساس شما خواهید آموخت که چگونه حتی از چند مشاهدات می توان به روش های ریاضی درست برای بهبود بیشتر تخمین های خود استفاده نموده و مدل های خود را با جزئیات و پیچیدگی بیشتر بهبود بخشید. در حال حاضر، ما فقط به ساده‌ترین روش‌های جایگزینی ممکن که امروزه در امنیت سایبری می تواند مورد استفاده قرار گیرد، اکتفا می کنیم.

۴-۱. یک تعویض ساده یک به یک

برای ارزیابی ریسک بهتر مسیری را با جایگزین کردن عناصری از روشی که اکثر کارشناسان امنیت سایبری قبلاً با آن آشنا هستند یعنی ماتریس ریسک آغاز کنیم. مانند رویکرد ماتریس ریسک فقط به قضاوت متخصصان موضوع در امنیت سایبری وابسته خواهیم بود و از قضاوت ذهنی و کارشناسانه خبرگان در مورد احتمال وقوع و تأثیر آن، همانطور که تحلیلگران اکنون با ماتریس ریسک انجام می دهند، استفاده می نماییم . در این رویکرد به جز اطلاعاتی که تحلیلگران امنیت سایبری ممکن است از قبل برای اطلاع از قضاوت های خود با ماتریس ریسک

[1] - Hubbard and Seiersen 2016,p.35-54
[2] - Rear Admiral Wayne Meyer,

استفاده کنند، به هیچ داده ای نیاز نیست. مانند قبل، کارشناسان می توانند از داده های مورد نظر خود برای اطلاع از آنچه در نهایت به یک قضاوت ذهنی می رسد استفاده کنند. ما فقط پیشنهاد می کنیم که به جای استفاده از مقیاس هایی مانند "بالا، متوسط، کم" یا ۱ تا ۵، کارشناسان یاد بگیرند که چگونه به طور ذهنی مقادیر واقعی پشت این مقیاس ها را ارزیابی کنند - یعنی احتمال و تأثیر پولی آن. در جدول ۱ نحوه جایگزینی هر عنصر از ماتریس ریسک با روشی که از احتمالات صریح استفاده می کند، ارائه شده است. روش پیشنهادی، مانند ماتریس ریسک، در واقع بیان دیگری از وضعیت فعلی عدم قطعیتی است که با آن روبرو هستیم و هنوز یک اندازه گیری مناسب را منعکس نمی کند که بتوان عدم قطعیت را بر اساس مشاهدات اضافی کاهش داد. ما صرفاً عدم اطمینان قبلی خود را بیان می کنیم. اما اکنون ما این سطح از عدم قطعیت را به گونه‌ای بیان کرده‌ایم که به ما امکان می‌دهد به طور واضح با خطر ارتباط برقرار کنیم و این عدم اطمینان را با اطلاعات جدید به روز کنیم. با ساده تر شدن موضوع ابتدا بخش هایی از این رویکرد را کنار هم می گذاریم و از اینجا شروع کنیم که چگونه کارشناس امنیت سایبری تخمین‌های ذهنی از احتمال را ارائه می‌کند.

جدول ۱- جایگزینی ساده ماتریس کمی به جای ماتریس ریسک

به جای:	جایگزین می نماییم :
رتبه بندی شانس یا احتمال وقوع در مقیاس ۱ تا ۵ یا کم تا زیاد. مثال: احتمال وقوع X ۲ است یا احتمال X متوسط است.	تخمین احتمال وقوع رویداد در یک دوره زمانی معین (به عنوان مثال، ۱ سال). مثال: ۱۰٪ احتمال دارد رویداد X احتمال دارد در ۱۲ ماه آینده رخ دهد.
رتبه بندی تاثیر وقوع رویداد در مقیاس ۱ تا ۵ یا کم تا زیاد. مثال: تاثیر رویداد X است ۲ یا تاثیر رویداد X متوسط است.	تخمین فاصله اطمینان ۹۰٪ برای ضرر پولی. مثال: اگر رویداد X رخ دهد، ۹۰٪ احتمال ضرر بین ۱ تا ۸ میلیون دلار وجود دارد.

۲-۴. کارشناس به عنوان ابزار

در رویکرد جایگزینی یک به یک از همان منبع اصلی برای تخمین ماتریس ریسک فعلی یعنی کارشناس امنیت سایبری استفاده می نماییم. همانطور که کارشناسان در حال حاضر احتمال و تاثیر را بر ماتریس ریسک مرسوم ارزیابی می کنند، آنها به سادگی می توانند این مقادیر را با استفاده از مقادیر معنی دار ارزیابی کنند. در مرحله بعد می توان اطلاعات خارجی تکمیلی را نیز به آن اضافه نمود. اما به سادگی ثبت وضعیت فعلی عدم قطعیت یک نقطه شروع مهم در هر مشکل اندازه گیری است. فقط باید یک ساختار اولیه با مراحل زیر را راه اندازی کنیم.

۱. فهرستی از خطرات را تعریف کنید. گزینه‌های مختلفی برای دسته‌بندی ریسک‌ها وجود دارد، اما در حال حاضر فقط بگوییم که این همان فهرستی است که در ماتریس ریسک معمولی ترسیم می‌شد.

۲. یک دوره زمانی خاص را که آن رویداد ریسک می تواند طی آن مشخص شود

تحقق یابد (به عنوان مثال، "یک نقض داده برای برنامه X در۱۲ ماه آینده، از دست دادن در دسترس بودن برای سیستم X به اندازه کافی برای متحمل شدن کاهش بهره وری در ۵ سال آینده رخ خواهد داد و غیره.

۳. برای هر ریسک، به طور ذهنی یک احتمال (۰٪ تا ۱۰۰٪) نسبت دهید. رویداد اعلام شده در زمان مشخص شده رخ می دهد (به عنوان مثال، "۱۰٪ وجود دارد این احتمال وجود دارد که در ۱۲ ماه آینده نقض اطلاعات سیستم X رخ دهد.

۴. برای هر ریسک، در صورتی که چنین رویدادی به عنوان "فاصله اطمینان ۹۰٪" (CI)[1] رخ دهد، به طور ذهنی محدوده ای برای زیان پولی تعیین کنید. این محدوده به اندازه کافی گسترده است که ۹۰٪ مطمئن باشید که ضرر واقعی در آن خواهد بود. محدوده اعلام شده (به عنوان مثال، اگر نقض داده در برنامه X وجود داشته باشد، سپس ۹۰٪ احتمال دارد که ضرری در فاصله ۱ میلیون و ۱۰ میلیون دلار وجود داشته باشد).

۵. در صورت امکان تخمین ها را از چندین متخصص دریافت کنید، اما اگر امکانپذیر نبود با نشستی مشترک و تلاش برای دستیابی به اجماع تخمین را تعیین نمایید. به سادگی لیست رویدادهای تعریف شده را ارائه دهید و اجازه دهید افراد جداگانه پاسخ دهند. اگر برخی از افراد پاسخ های بسیار متفاوتی نسبت به دیگران می دهند، بررسی کنید که آیا آنها مشکل را متفاوت تفسیر می کنند یا خیر. به عنوان مثال، اگر یک نفر بگوید احتمال وقوع چیزی در یک سال ۵٪ است، و دیگری می گوید ۱۰۰٪ احتمال دارد هر روز اتفاق بیفتد، سپس آنها احتمالاً سؤال را متفاوت تفسیر کرده اند (مواردی از این دست بر اساس تجربه متناوباً اتفاق می افتند[2]) . اما تا زمانی که آنها حداقل سؤال را به طور مشابه تفسیر می کنند، به سادگی پاسخ های خود را میانگین بگیرید. یعنی متوسط همه

[1] - Confidence Interval

[2] - Hubbard and Seiersen 2016,p.38

احتمالات رویداد برای محاسبه یک احتمال محاسبه نمایید. همچنین میانگین همه کران پایین ها و میانگین همه کران بالا را برای تولید کران پایین و بالا استفاده کنید. البته برخی ممکن است به ایده ارزیابی ذهنی احتمالات اعتراض کنند. برخی از تحلیلگرانی که مشکلی برای گفتن اینکه احتمال ۴ در مقیاس ۱ تا ۵ یا متوسط در مقیاس شفاهی است، مشکلی ندارند استدلال خواهند کرد که الزاماتی برای احتمالات کمی وجود دارد که کمی سازی را غیرممکن می کند. به نوعی در مسائلی که در آنها مشکلی در استفاده از روش‌های مبهم‌تر وجود ندارد، بیشتر با بن بست در تلاش برای بیان احتمالات معنادار روبرو هستند. البته این یک سوء تفاهم رایج است. همانطوری که قبلاً بیان شد استفاده از یک احتمال ذهنی یک متخصص برای تعیین مقدار احتمال یا عدم قطعیت پیشین داری جایگاه معتبر ریاضی است. در واقع، مشکلاتی در آمار وجود دارد که تنها با استفاده از استفاده از احتمال پیشین قابل حل هستند و اینها در واقع همان موقعیت هایی هستند که بیشترین ارتباط را با تصمیم گیری در هر زمینه ای از جمله امنیت سایبری دارند. علاوه بر این روش هایی برای بهبود احتمال محاسبه شده می تواند مورد استفاده قرار گیرد که می توان از آن به عنوان ارزیابی احتمال کالیبره شده یاد نمود و تحقیقات زیادی نیز وجود دارد که اعتبار این رویکرد را تایید می کند. در حال حاضر، فقط به این اکتفا می نماییم که اکثر متخصصان می توانند برای ارزیابی ذهنی احتمالات آموزش ببینند و این مهارت به طور عینی قابل اندازه گیری است. به یاد داشته باشید، اگر نگرانی اصلی در مورد استفاده از روش‌های احتمالی کمبود داده است، پس شما نیز فاقد داده برای استفاده از روش‌های غیر کمی هستید. همانطور که بیان کردیم، هر دو روش تاکنون بر اساس یک منبع داده یعنی نظر متخصصان امنیت سایبری بنا نهاده شده اندو ما نمی‌توانیم فرض کنیم که با استفاده از روش‌های کیفی از هر اشتباهی که ممکن است از طریق کاربرد احتمالات کمّی به تصمیم خود وارد کنیم، قابل اجتناب است. می توان با استفاده از روش‌هایی دو منبع دیگر خطا در قضاوت یعنی درجه بالایی از ناسازگاری کارشناسان، و تمایل به اشتباهات استنتاج رایج در هنگام تفکر احتمالی را بهبود داد که در ماتریس ریسک معمولی به این منابع خطا پرداخته نمی شود.

۳-۴. عملیات ریاضی عدم قطعیت

استفاده از محدوده ها برای نشان دادن عدم قطعیت شما به جای مقادیر دقیق نقطه ای غیرواقعی، به وضوح مزایایی دارد. وقتی به خود اجازه می دهید از محدوده ها و احتمالات استفاده کنید، واقعاً لازم نیست چیزی را که نمی دانید به طور واقعی فرض کنید. اما مقادیر دقیق این مزیت را دارند که جمع، تفریق، ضرب و تقسیم در یک صفحه گسترده ساده هستند. اگر هر نوع ضرر را دقیقاً می دانستید، محاسبه کل ضرر آسان بود. از آنجایی که ما فقط برای هر یک از این محدوده‌ها داریم، باید از روش‌های مدل‌سازی احتمالی برای انجام محاسبات استفاده کنیم.

حال سوال اینجاست که چگونه در یک صفحه گسترده جمع، تفریق، ضرب و تقسیم کنیم وقتی مقادیر دقیق نداریم و فقط محدوده داریم؟ خوشبختانه، یک راه حل عملی و اثبات شده وجود دارد، و می توان آن را بر روی هر کامپیوتر شخصی مدرن انجام داد این روش شبیه سازی مونته کارلو[1] نام دارد. شبیه سازی مونت کارلو از یک کامپیوتر برای تولید تعداد زیادی سناریو بر اساس احتمالات برای ورودی ها استفاده می کند. برای هر سناریو، مقدار خاصی به طور تصادفی برای هر یک از متغیرهای ناشناخته تولید می شود. سپس این مقادیر خاص وارد یک فرمول برای محاسبه خروجی برای آن سناریو می شوند. این روند معمولاً برای هزاران سناریو ادامه دارد. در دهه ۱۹۴۰، برخی از ریاضیدانان و دانشمندان شروع به استفاده از چنین شبیه سازی هایی از هزاران آزمایش تصادفی برای کمک به حل برخی مسائل ریاضی بسیار سخت کردند. استانیسلاو اولام[2]، جان فون نویمان[3] و نیکلاس متروپلیس[4] راهی برای استفاده از این روش در کامپیوترهای ابتدایی موجود در آن زمان برای کمک به حل مسائل ریاضی مربوط به ساخت اولین بمب اتمی ایجاد کرده بودند. آنها دریافتند که اجرای تصادفی هزاران کارآزمایی راهی برای بررسی احتمالات نتایج مختلف زمانی است که یک مدل دارای تعدادی ورودی بسیار نامشخص است. به پیشنهاد متروپلیس، اولام این روش مبتنی بر کامپیوتر برای تولید سناریوهای تصادفی را به افتخار عموی اولام، که یک قمارباز بود و نیز به افتخار مونت کارلو، یک مرکز معروف قمار بازی است، نامگذاری کرد. اکنون، با مزیت قدرت محاسباتی بیشتر (به راحتی میلیاردها بار) تقریباً با هر معیاری، بیشتر از آنچه در پروژه منهتن موجود بود، شبیه‌سازی‌های مونت کارلو برای شبیه‌سازی مدل‌های ریسک در نیروگاه‌ها، زنجیره‌های تامین، بیمه، ریسک‌های پروژه، ریسک‌های مالی، و امنیت سایبری استفاده شده‌اند. اگر تجربه ای در مورد شبیه سازی مونت کارلو ندارید، احتمالاً ساده تر از آن چیزی است که فکر می کنید. نویسندگان و بسیاری از کارکنان آنها به طور معمول شبیه سازی مونت کارلو را بر روی انواع مشکلات تجاری عملی اعمال می کنند. دیده‌ایم که بسیاری از افرادی که در ابتدا از ایده استفاده از شبیه‌سازی‌های مونت کارلو ناراحت بودند، در نهایت پس از دستکاری خود ابزارها، به حامیان مشتاق تبدیل شدند.

بیایید با یک مشکل بسیار ساده شروع کنیم و ابزارهایی برای حل آن ارائه کنیم. فرض کنید مجموعه‌ای از رویدادهای احتمالی دارید که ممکن است در یک دوره یک ساله مشخص رخ دهند. هر رویداد دارای یک احتمال اختصاص داده شده است و در صورت وقوع، طیفی از ضررهای احتمالی را دارد. بیایید فرض کنیم که برخی از رویدادها احتمال ۱٪ و شاید برخی از آنها احتمال بیش از ۱۰٪ داشته باشند. در هر سال ممکن است هیچ رویداد زیان قابل توجهی رخ ندهد و همچنین ممکن است چندین رویداد رخ دهد. حتی ممکن است یک رویداد

---

[1] - Monte Carlo Simulation
[2] - Stanislaw Ulam,
[3] - John von Neumann
[4]- Nicholas Metropolis

یکسان چندین بار در یک سال اتفاق بیفتد. راه حلی برای آن وجود دارد، اما در حال حاضر ما آن را ساده نگه می داریم و فقط یک رویداد را به عنوان یک یا یا نتیجه ای که بیش از یک بار در سال اتفاق نمی افتد مدل می کنیم. ماتریس ریسک به هر حال این تمایز را ایجاد نمی‌کند (و چند مورد دیگر را که بعداً معرفی خواهیم کرد را از دست می‌دهد)، بنابراین این کمک می‌کند تا مثال را به جایگزینی یک به یک نزدیک‌تر نگه داریم. ما این فرصت را خواهیم داشت که به جزئیات بیشتر در مورد این نوع بپردازیم

مدل سازی در آینده در کتاب. اما برای کمک به شروع کار، چند مثال ساده در یک صفحه گسترده اکسل ارائه کرده ایم که می توان آنها را از www.howtomeasureanything.com/cybersecurity دانلود کرد. با داشتن این اطلاعات و برخی از محتوای دقیق‌تری در فصل های بعد ارائه می شود، باید بتوانید عدم قطعیت خود را مدل کنید و به سؤالاتی مانند "احتمال اینکه در سال آینده بیش از X را به دلیل حمله سایبری از دست دهیم چقدر است؟" برای انجام این کار ما هزاران سناریو را برای هر خطر شبیه سازی خواهیم کرد. ما فقط باید در هر سناریو مشخص کنیم که آیا رویدادی برای هر نوع ریسک رخ می دهد یا خیر و در صورت وقوع، تاثیر آن چه خواهد بود.

۴-۴. مقدمه ای بر ایجاد رویدادها و تاثیرات تصادفی

ابتدا با این مسئله شروع می کنیم که آیا رویداد برای یک ریسک در یک سناریوی واحد رخ داده است یا خیر. برای شبیه سازی اینکه آیا یک رویداد خاص رخ می دهد یا نه، می توانیم به طور تصادفی اعداد صفر و یک را تولید نماییم. بر این اساس اعداد ۱ نشان دهنده و قوع و اعداد ۰ نشان دهنده عدم وقوع رویداد مورد نظر هستند. یک "۱" در صورت وقوع و یک "۰" در صورت عدم وقوع، که در آن احتمال "۱" برابر با احتمال اعلام شده رویداد است، تولید کنیم. در اکسل می توانیم این را به صورت زیر بنویسیم:

=if (rand () <probability of event,1,0)

برای مثال، اگر احتمال رویداد ۰.۱۵ باشد، این معادله خواهد بود

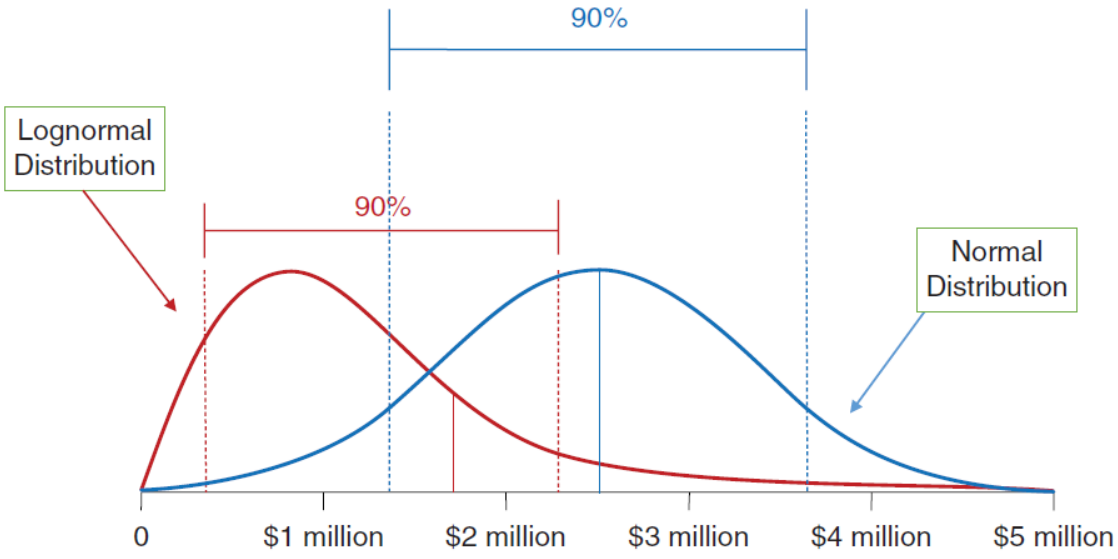
٪۱۵ مواقع "۱" (به معنی وقوع رویداد) تولید کنید. در اکسل، هر بار که این را دوباره محاسبه کنید (F9 را فشار دهید)، نتیجه متفاوتی خواهید دید. اگر این کار را هزار بار انجام دهید، می بینید که این رویداد حدود ۱۵۰ بار رخ می دهد. توجه داشته باشید که این برای هر ریسک فردی است که در شبیه سازی خود فهرست می کنید. بنابراین اگر شما ۱۰۰ ریسک با احتمالات مختلف دارید و ۱۰۰۰ سناریو را اجرا می کنید، این فرمول کوچک ۱۰۰۰۰۰ بار اجرا می شد. برای تأثیر، ما نه تنها باید «۰» یا «۱»، بلکه مقادیری پیوسته از اعداد را ایجاد کنیم. این کار را می توان با استفاده از یکی از "توابع احتمال معکوس" اکسل انجام داد. برخی از توابع احتمال در اکسل احتمال یک رویداد معین را در قالب یک توزیع احتمال خاص در اختیار میگذارند. به عنوان مثال،

normdist(x,mean,stddev,1) احتمال تجمعی یک توزیع نرمال در نقطه x را با میانگین داده شده و انحراف معیار معین را محاسبه می نماید. از طرف دیگر، تابع احتمال معکوس، مقدار x را با یک احتمال به شما می گوید. در اکسل، تابع احتمال معکوس برای یک توزیع نرمال است با فرمول زیر محاسبه می شود:

= norminv (probability, mean, standard deviation)

لازم به ذکر است که در نسخه‌های اخیر اکسل از تابع norm.inv() نیز استفاده می شود، لیکن norminv() همچنان کار می کند) اگر از تابع rand() در اکسل به جای عبارت probability استفاده نمایید، داده های تصادفی مربوط به متغیر تصادفی x دارای توزیع احتمال نرمال با میانگین و انحراف معیار تعریف شده را تولید می نماید. اما در واقع کمیت های مزبور چندان شهودی نیست تا یک متخصص خبره بتوان تخمین بزند. بهتر است همانطور که قبلاً توضیح داده شد فقط از متخصص یک فاصله اطمینان ۹۰ درصدی بخواهیم. این می تواند برای محاسبه پارامترهای مورد نیاز مانند میانگین و انحراف استاندارد بر اساس کران بالا (UB) و کران پایین (LB) برای توصیف طیفی از تلفات بالقوه ارائه شده توسط متخصص استفاده شود. ما قصد داریم آن محدوده را به یک توزیع احتمال از نوع خاصی تبدیل کنیم که اغلب از آن استفاده خواهیم کرد. این توزیع احتمال "lognormal" نام دارد. اگر فرض کنیم که x یک متغیر تصادفی باشد در این صورت این متغیر زمانی توزیع احتمال لُگ نرمال دارد که لگاریتم x (یا بعبارت ریاضی تر $\ln(x)$) دارای توزیع نرمال است. هر چند در حالت هایی شکل توزیع این دو شبیه یکدیگر است و زنگوله وار است ولی در بسیاری از حالت ها شکل این دو می تواند متفاوت باشد همانطوری که در شکل ۳ نمایش داده شده است.

شکل ۳ – مقایسه نمودار توزیع احتمال نرمال و لُگ نرمال



مأخذ: (Hubbard and Seiersen 2016,p.41)

نمودار آبی که نشان دهنده توزیع نرمال است که به شکل یک زنگوله می باشد. لیکن توزیع لُگ نرمال بر خلاف توزیع نرمال، کج[1] یا "چوله" [2]است. توزیع لُگ نرمال نمی تواند مقدار صفر یا منفی ایجاد کند، اما دارای یک دنباله به سمت راست است که امکان وقوع مقادیر بسیار بزرگ را فراهم می کند.

برای بیان هر چه بهتر نحوه شبیه سازی فرآیند تصادفی وقوع ضررهای ناشی از وقوع یک پدیده نامطلوب ابتدا لازم است که مبانی آماری مورد نیاز تبیین شود. با توجه به اینکه در نظر داریم وقوع ضرر را در یک بازه بین مقدار حداقل و حداکثر و با احتمال وقوع ۹۰٪ حالت ها در نظر بگیریم در ادامه چارچوب مورد نیاز ارائه می شود.

۴-۵. تحلیل بازه ۹۰٪ اطمینان[3] در توزیع نرمال

فرض کنیم که متغیر تصادفی y دارای توزیع نرمال با میانگین μ_y و انحراف معیار σ_y است. همچنین فرض کنیم که دو مقدار از این توزیع را به عنوان حد پائین و حد بالا به ترتیب y_L و y_U را در دست داریم و برداشت ما این است که مقادیر y در ۹۰٪ حالات بین دو مقدار یعنی در بازه (y_L, y_U) قرار می گیرد. با توجه به متقارن بودن توزیع نرمال و با نظر به اینکه ۱۰٪ حالت ها متغیر خارج از این بازه قراردارد نتیجه می گیریم که فقط۵٪ احتمال دارد که متغیر بیشتر از y_U و یا کمتر از y_L باشد. از سوی دیگر بنابر تقارن توزیع نرمال میانگین توزیع وسط بازه (y_L, y_U) قراردارد و به عبارت ریاضی داریم :

$$\mu_y = \frac{y_L + y_U}{2}$$

همچنین با توجه به توضیحات فوق داریم:

$$y_{5\%} = y_L \text{ و } y_{95\%} = y_U$$

از سوی دیگر بنابر خصوصیات توزیع نرمال متغیر $Z = \frac{y-\mu_y}{\sigma_y}$ دارای توزیع نرمال استاندارد است. یعنی میانگین آن صفر و انحراف معیار آن ۱ است و جالبتر اینکه $Z_{95\%} = \frac{y_{95\%}-\mu_y}{\sigma_y}$ نیز بر قرار است. بر این اساس و با توجه به اینکه از جدول توزیع نرمال می دانیم که $Z_{95\%} = 1.644853627 \cong 1.645$. بدین ترتیب و با استفاده از روابط $Z_{95\%} = \frac{y_U-\mu_y}{\sigma_y}$ و $\mu_y = \frac{y_L+y_U}{2}$ می توانیم انحراف معیار توزیع تصادفی y را به شرح زیر محاسبه نماییم:

$$Z_{95\%} = \frac{y_L - \frac{y_L + y_U}{2}}{\sigma_y} = \frac{y_L - y_U}{2 \times \sigma_y} \Longrightarrow \sigma_y = \frac{y_L - y_U}{2 \times Z_{95\%}} = \frac{y_L - y_U}{2 \times 1.645} = \frac{y_L - y_U}{3.29}$$

با توجه به نتایج فوق الذکر می توانیم قضیه زیر بیان نماییم :

---

[1] - lopsided
[2] - skewed
[3] - Confidence Interval (CI)

قضیه : فرض کنیم که متغیر تصادفی y *دارای توزیع نرمال با میانگین* μ_y *و انحراف معیار* σ_y *است. همچنین فرض کنیم که دو مقدار از این توزیع را به عنوان حد پائین و حد بالا به ترتیب* y_L *و* y_U *را در دست داریم و برداشت ما این است که مقادیر* y *در ۹۰٪ حالات بین دو مقدار یعنی در بازه* (y_L, y_U) *قرار می گیرد. در این صورت میانگین* $\mu_y = \frac{y_L+y_U}{2}$ *و انحراف معیار* $\sigma_y = \frac{y_L-y_U}{3.29}$ *است.*

حال اگر متغیر تصادفی x دارای توزیع لُگ نرمال داشته باشد در این صورت متغیر $y = \ln(x)$ دارای توزیع نرمال است. بر این اساس برای تولید اعداد تصادفی که دارای توزیع لُگ نرمال هستند کافی است که لگاریتم این اعداد را تحت توزیع نرمال تولید نموده و اعداد بدست آورده را به توان e برسانیم. از همین طریق می توان با دستور زیر در اکسل اعداد تصادفی با توزیع لُگ نرمال را تولید نمود :

$$= lognorm.inv(rand(), mean\ of\ \ln(x), standard\ deviation\ of\ \ln(x))$$

لذا با توجه به روابط بدست آمده قبلی می توان مقادیر ضرر(که در ابتدا فرض نمودیم دارای توزیع لُگ نرمال هستند) را که انتظار داریم در ۹۰٪ حالات بین دو مقدار UB و LB باشند را می توان با دستور زیر می توان به صورت تصادفی تولید نمود:

$$= lognorm.inv(rand(), \frac{(\ln(UB)+\ln(LB))}{2}, \frac{(ln(UB)-ln(LB))}{3.29})$$

لازم به ذکراست که هرچند نرم افزار اکسل قادر به انجام محاسبات فوق است و عملاً به دلیل خصوصیات صفحه گسترده کاربر پسند می باشد لیکن به دلیل خصوصیات ذاتی که دارد از جمله اینکه مقادیر را در سلول های مربوطه به نمایش می گذارد که خود نیازمند تخصیص حافظه و نیز انجام عملیات مربوط به بروز نمودن سلول هاست برای پردازش های سنگین عملاً کند بوده که موجب می شود در شبیه سازی های با حجم بالا با مشکل روبرو شویم. البته امکان استفاده از زبان VBA برای ماکرو نویسی در اکسل و تمام نرم افزار های مایکروسافت آفیس وجود دارد که در صورتی که در برنامه نمایش لحظه ای مقادیر سلول ها صورت نگیرد نرم افزار با سرعت بالاتری در پشت صفحه انجام داده و به یک باره نتایج را نمایش می دهد که این امر می توان انجام محاسبات را به نحو قابل توجهی افزایش دهد. البته نرم افزار شبیه سازی بر پایه اکسل مانند @Risk و Crystal Ball وجود دارند که به خوبی می توانند انواع شبیه سازی ها و بهینه سازی ها را در محیط اکسل با سرعت بالایی انجام دهند. با این حال تجربه نویسنده این نوشتار طی سالهای متمادی در زمینه مدل سازی حوزه ریسک مالی و نیز تدریس مدیریت در نظام بانکی کشور مشغول به فعالیت بوده نشان می دهد که یکی از نرم افزارهایی که نیازهای مدل سازان حوزه ریسک برای انجام محاسبات پیچیده و به ویژه شبیه سازی را برآورده نماید نرم افزار معروف

MATLAB است. نام این نرم افزار که برگرفته شده از عبارت انگلیسی MATrix LABratory به معنی لابراتور یا آزمایشگاه ماتریس است نشاندهنده قدرت مزیت آن در پردازش ماتریسی است. به همین دلیل است که این نرم افزار قادر است شبیه سازی ها حجیم را به خوبی انجام دهد زیرا با استفاده از توانایی های عملیات ماتریس این نرم افزار است میلیون ها عملیات را براحتی و در زمان بسیار کم انجام دهد. همچنین با بهره گیری از توان برنامه نویسی در قالب m file این نرم افزار کاربر را قادر می سازد که برنامه های بسیار قوی و کاربردی را در حجم کمی نوشته و سپس به اجرا گذارد. برای این منظور و به دلایلی که به اختصار بیان شد برای انجام مثال های کاربردی مرتبط با این نوشتار از این نرم افزار شده و در ادامه نیز به نحو مقتضی به آن پرداخته می شود.

۴-۶. شبیه سازی پیامد وقوع در بازه اطمینان ۹۰٪

مسئله۱ : فرض کنید بر اساس بررسی انجام شده برای رخداد امنیت سایبری که آن را Event 1 می نامیم ضرر وقوع با اطمینان ۹۰٪ بین ۳۰۰۰ تا ۱۰۰۰۰ واحد پولی است. با این فرض مقدار ضرر یک متغیر تصادفی با توزیع لُگ نرمال باشد در نظر داریم که فرآیند وقوع ضرر را با استفاده از روش مونت کارلو شبیه سازی نماییم.

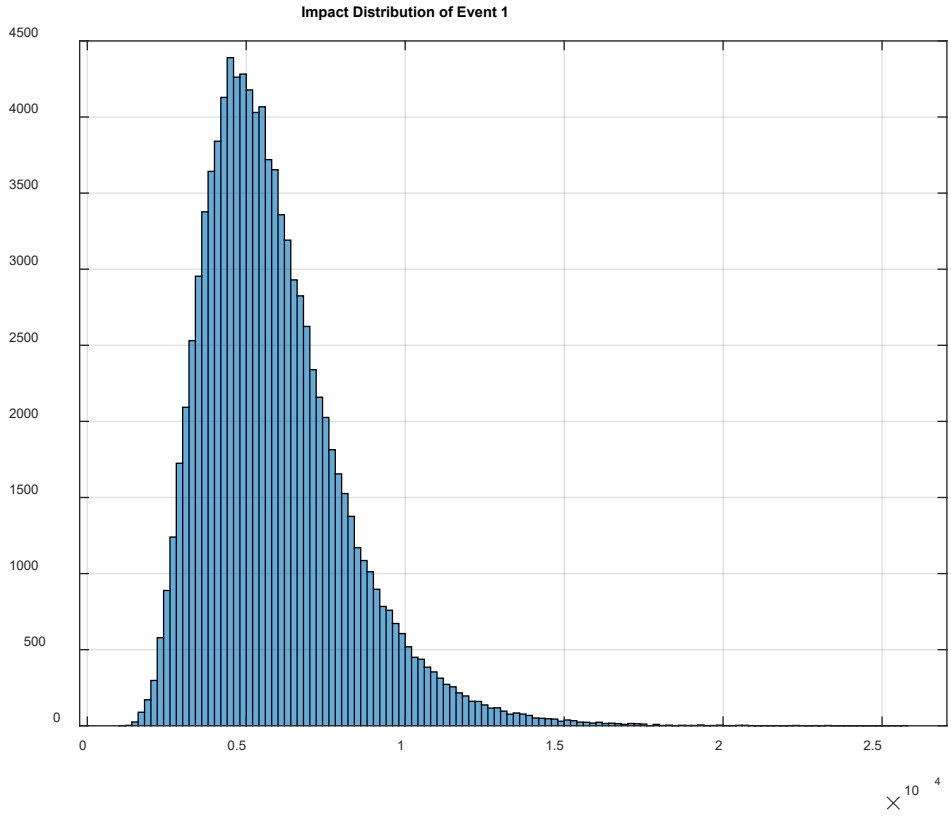
را حل : برای شبیه سازی از نرم افزار MTLAB استفاده کرده و وقوع ضرر با توزیع لُگ نرمال برای ۱۰۰ بار آزمایش نموده و توزیع ضرر را شبیه سازی می نماییم. برای این منظور از کد برنامه زیر تحت نرم افزار مزبور استفاده می نماییم:

شکل ۴- کد برنامه MATLAB برای تولید اعداد تصادفی در بازه (۱۰۰۰۰ ۳۰۰۰) با اطمینان ۹۰٪ و با توزیع لُگ نرمال

```
clear;
clc;
m=1000000;
Impact_LB=3000;
Impact_UB=10000;
Impact_mean=(log(Impact_UB)+log(Impact_LB))/2;
Impact_std=(log(Impact_UB)-log(Impact_LB))/3.29;
A=Impact_mean*ones(m,1);
B=Impact_std*ones(m,1);
Impact=random('Lognormal',A,B);
histogram(Impact)
title('Impact Distribution of Event 1 ')
grid on
```

همانطوریکه مشخص است کد برنامه فوق بسیار کم حجم است و از هیچگونه حلقه for و یا if که زمان زیادی را برای محاسبه صرف می نماید استفاده نشده است. نمودار هیستوگرام برنامه فوق که در ادامه آورده می شود نیز به صورت واضحی توزیع آماری متغیر تصادفی مورد نظر را نیز نشان می دهد.

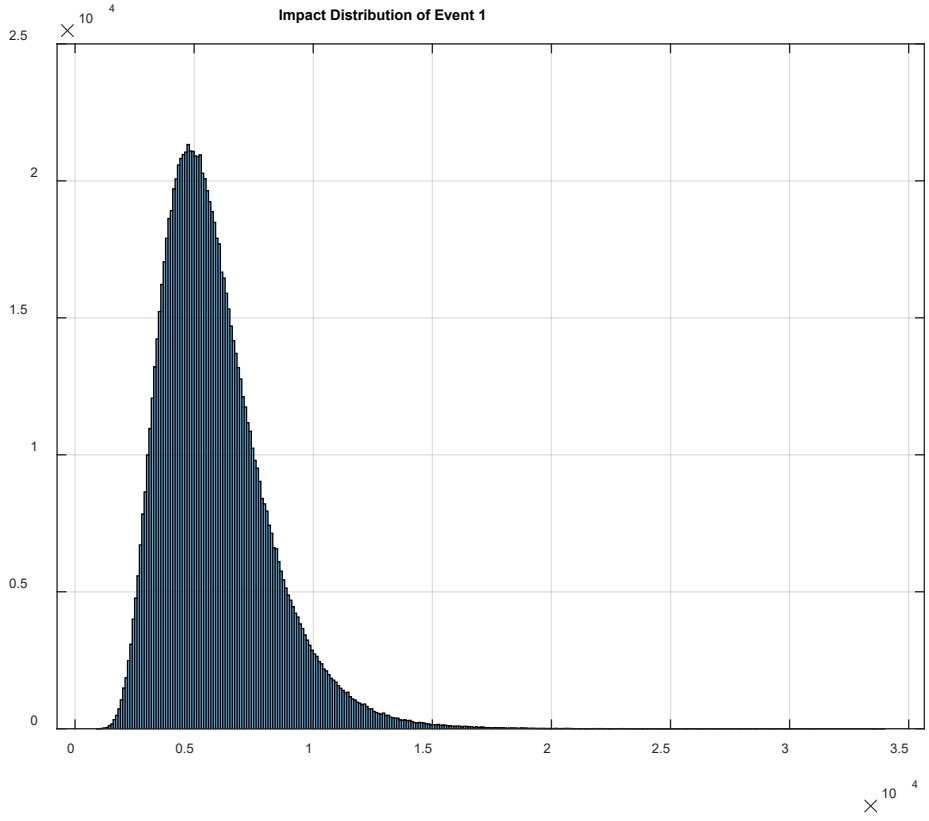
شکل ۵- نمودار هیستوگرام شبیه سازی مونت کارلو برای ۱۰۰۰۰۰ هزار حالت توزیع اعداد تصادفی در بازه (۱۰۰۰۰ ۳۰۰۰) با اطمینان ۹۰٪ و توزیع لُگ نرمال



با وارد نمودن کد برنامه MATLAB برای چندک[1] ٪۹۵ و ۵٪ به خوبی مشخص می شود که اعداد بدست آمده با مقادیر ۱۰۰۰۰ و ۳۰۰۰ تفاوت بسیار ناچیزی دارند. مقادیر مزبور که توسط نرم افزار محاسبه شده است به ترتیب عبارتند از ۱۰۰۰۷ و ۲۹۹۸/۲ . حال اگر تعداد شبیه سازی را یکصد هزار حالت به یک میلیون حالت ارتقاء بخشیم انتظار می رود که تصویر واقعی تری از فرآیند تصادفی مزبور به دست آوریم. این کار با تغییر فقط یک پارامتر از ۱۰۰۰۰ به ۱۰۰۰۰۰۰ انجام شده و هیستوگرام زیر بدست آمد. همچنان که در شکل به وضوح دیده می شود نمودار بسیار نرم تر و واضح تر از حالت قبلی است.

[1] - Quantile

شکل ۶- نمودار هیستوگرام شبیه سازی مونت کارلو برای ۱۰۰۰۰۰ هزار حالت توزیع اعداد تصادفی در بازه (۱۰۰۰۰ ۳۰۰۰) با اطمینان ۹۰٪ و توزیع لُگ نرمال



شایان ذکر است که اعداد فوق فقط نشان دهنده پیامد وقوع پدیده هستند و برای مدل سازی توزیع ضرر لازم است فرآیند وقوع نیز شبیه سازی شود. برای این منظور به دو طریق کلی عینی مبتنی بر[۱] مشاهدات تاریخی[۲] و یا بر اساس برداشت ذهنی[۳] می تواند مورد استفاده قرار گیرد. در رویکرد اول نیاز به اطلاعات تاریخی وقوع پدیده مورد نظر را دارد البته در بسیاری از حالات ممکن است اطلاعات کاملی در دست نباشد لیکن در صورت وجود می توان احتمال وقوع را برآورد نمود. در ساده ترین مدل توزیع وقوع توزیع برنولی[۴] فرض می شود که در آن متغیر پاسخ[۵] دو حالت وقوع(که معمولاً با ۱ نمایش داده می شود) و حالت عدم وقوع(که با ۰ نمایش داده می شود) را دارد. این فرآیند به ظاهر ساده ولی کلیدی در مدل های و سیستم های احتمالاتی بسیار کاربرد دارد. به زبان ساده این فرآیند مانند پرتاب یک سکه است که احتمال خط در آن p و احتمال شیر آمدن $1-p$ است. از نظر محاسباتی بر اساس مبانی آمار و احتمالات، برآورد p با تقسیم تعداد وقوع پدیده مورد نظر در یک دوره

[1] - Objective
[2] - Historical Observations
[3] - Subjective
[4] - Bernoulli Distribution
[5] - Response Variable

زمانی مشخص(یا فارغ از چارچوب زمانی) بر کل حالات اتفاق افتاده بدست می آید. به طور مثال اگر در ۳۶۵ روز فعالیت یک بانک ۱۰ بار(طی ۱۰ روز) شبکه بانک مورد تهاجم و دسترسی غیر مجاز اطلاعات[1] گرفته است احتمال وقوع این پدیده نامطلوب طی یکسال بالغ بر $p = \frac{10}{365} \cong 0.027$ خواهد بود. برای محاسبه احتمال وقوع مزبور باید به چند نکته توجه نمود که در ادامه آورده می شود.

۱- مقدار احتمال p طی مشاهدات مختلف می تواند تغییر نماید و لذا یک مقدار برآوردی است. لیکن بنابر مبانی علم آمار با افزایش تعداد مشاهدات می تواند به یک حدی میل نماید. به هر تقدیر با افزایش مشاهدات دقت برآورد افزایش می یابد.

۲- مقدار p یک متغیر تصادفی است که البته بر اساس قضیه بیز و روش بیزین[2] امکان بهبود برآورد وجود دارد .در این ارتباط استفاده از توزیع بتا برای تخمین و بروز نمودن مقدار متغیر مزبور با استفاده از مشاهدات جدید وجود دارد که بعداً به آن پرداخته خواهد شد.

۴-۷. شبیه سازی ضرر با فرض وقوع با توزیع یکنواخت

بر اساس مطالب فوق الذکر می خواهیم که مسئله ۱ را با اضافه نمودن احتمال وقوع رخداد کاملتر نموده و توزیع ضرر را با استفاده از شبیه سازی مونت کارلو ایجاد نماییم. برای این منظور مسئله ۲ به شرح زیر تعریف می نماییم.

مسئله ۲: فرض کنیم که اطلاعات موضوع مسئله برقرار باشد و بررسی های انجام شده در ارتباط احتمال وقوع رخداد دلالت بر این دارد که مقدار احتمال وقوع p طی یک دوره یک ساله بالغ بر ۵٪ است. با فرض اینکه وقوع رویداد از توزیع برنولی پیروی نماید توزیع ضرر وقوع رخداد Event 1 را طی یکسال با استفاده از شبیه سازی مونت کارلو بدست آورید.

حل : در کد برنامه MATLAB اطلاعات جدید را بروز نموده و شبیه سازی فرآیند برنولی را نیز اضافه می نماییم. بر این اساس کد برنامه به شرح زیر توسعه می یابد. نمودارهای هیستوگرام توزیع ضرر، پیامد و نیز وقوع خروجی این برنامه می باشند نیز در ادامه آورده شده است.

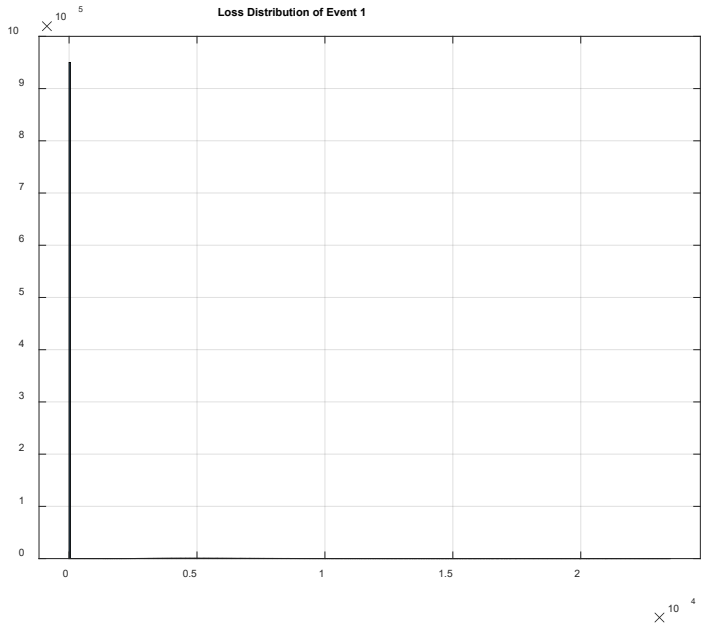
[1] - Data Breach

[2] - Bayesian Theory

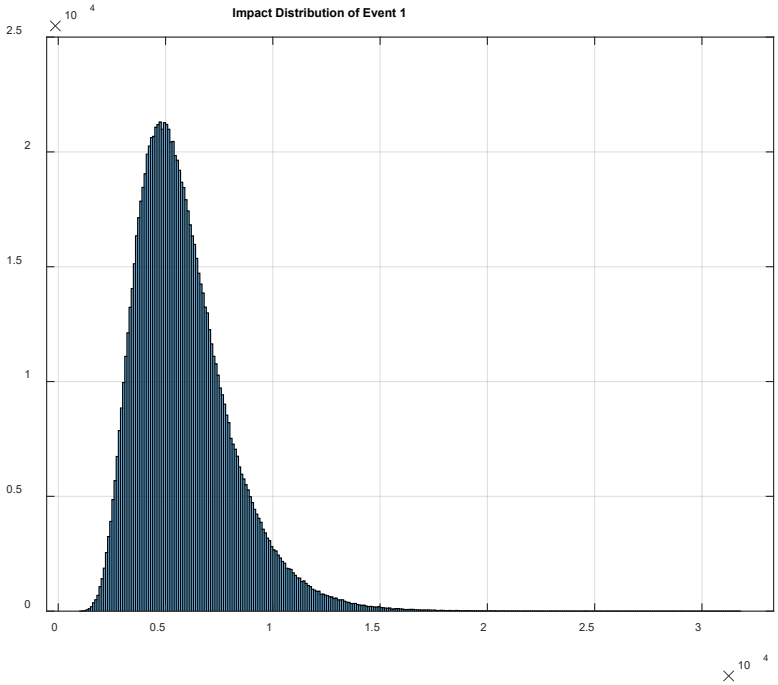
شکل ۷- کد برنامه MATLAB برای شبیه سازی وقوع پدیده Event 1

```
clear;
clc;
m=1000000;
Impact_LB=3000;
Impact_UB=10000;
p=0.05;
Impact_mean=(log(Impact_UB)+log(Impact_LB))/2;
Impact_std=(log(Impact_UB)-log(Impact_LB))/3.29;
A=Impact_mean*ones(m,1);
B=Impact_std*ones(m,1);
C=p*ones(m,1);
Impact=random('Lognormal',A,B);
Incident=random('Binomial',ones(m,1),C);
Loss=Impact.*Incident;
figure(1)
histogram(Loss)
title('Loss Distribution of Event 1 ')
grid on
figure(2)
histogram(Impact)
title('Impact Distribution of Event 1 ')
grid on
figure(3)
histogram(Incident)
title('Incident Distribution of Event 1 ')
grid on
```

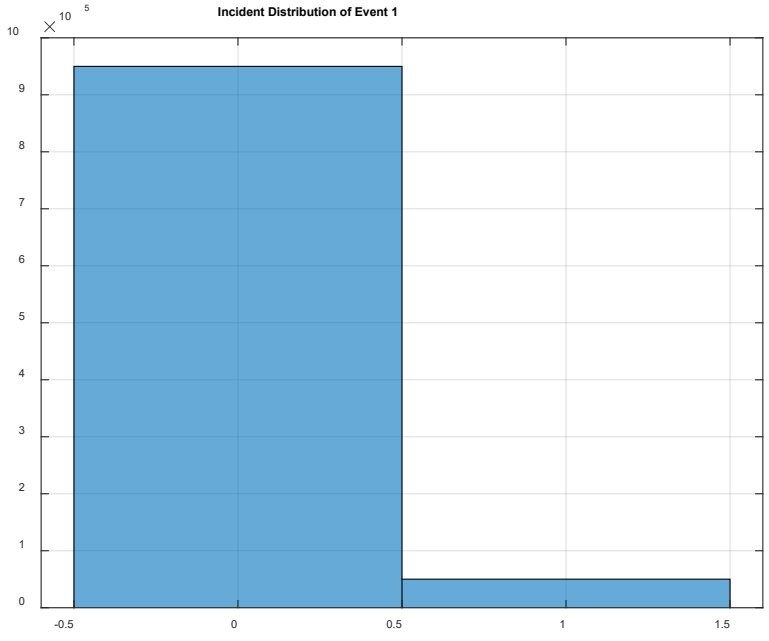
شکل ۸- توزیع ضرر با فرض وقوع با توزیع یکنواخت و پیامد با توزیع لُگ نرمال



شکل ۹- توزیع پیامد با توزیع لُگ نرمال



شکل ۱۰- توزیع وقوع با توزیع یکنواخت



۸-۴. شبیه سازی ضرر با فرض وقوع با توزیع پواسن با نرخ وقوع ثابت λ

همانطوری که از نمودار توزیع ضرر مشخص است به دلیل اینکه توزیع وقوع رخداد فقط دو حالت صفر و یک را در بر می گیرد و مقدار احتمال وقوع نیز بسیار کم است. لذا عملاً توزیع ضرر حالت های اکستریم را به خوبی نمایش نمی دهد. دلیل دیگر اینکه برای هر بار تکرار[1] که در برگیرنده دوره یک ساله است فقط حداکثر یک رخداد می تواند اتفاق بیفتد در حالیکه بواقع امکان وقوع بیش از یک مورد در سال نیز وجود دارد که البته به دلیل محدودیت ذاتی مدل این موضوع در نظر گرفته نمی شود. بر این اساس لازم است که مدل ساده برنولی به یک مدل پیشرفته تر گسترش یابد که امکان وقوع بیش از یک اتفاق نامطلوب در طی یک سال را فراهم آورد. این توزیع پواسن[2] نام دارد. به واقع توزیع پواسن مدل توسعه یافته توزیع برنولی است که البته بر اساس آمار ریاضی کاملاً قابل اثبات است که از چارچوب این نوشتار خارج است. لیکن به همین بسنده می کنیم که توزیع پواسن احتمال وقوع n رخداد را در یک دوره زمانی فراهم می کند. پدیده مورد نظر دارای متوسط نرخ وقوع ثابت λ در یک دوره زمانی مشخص است. برای این منظور احتمال وقوع n رخداد طی دوره t از رابطه زیر محاسبه می شود.

$$P(n) = \frac{(\lambda t)^n e^{-\lambda t}}{n!}$$

حال اگر بر اساس توزیع برنولی پارامتر p را برآورد شده باشد و دوره زمانی نیز مشخص باشد با ضرب این دو می توان لاندای توزیع پواسون را بدست آورد[3]. حال با در دست داشتن نسبت وقوع ۰.۰۵ در سال و با فرض اینکه دوره زمانی یکساله یعنی ۳۶۵ روز باشد و در هر روز نیز فقط یک اتفاق نامطلوب به وقوع به پیوندد نتیجه می گیریم نرخ وقوع در یک سال برابر حاصل ضرب ۳۶۵ در ۰.۰۵ یعنی به طور متوسط ۱۸/۲۵ رخداد در سال است. لذا می توان ادعا کنیم که پارامتر لاندای توزیع پواسن ۱۸/۲۵ است یعنی به عبارت ریاضی تر $\lambda = 18.25$. حال اگر مدل وقوع را به توزیع پواسن گسترش دهیم کد برنامه MATLAB و خروجی های آن به شرح ادامه خواهد بود. همانطوری که از نمودارهای هیستوگرام مشهود است تفاوت مدل بهبود یافته مبتنی بر توزیع وقوع پواسن با مدل اولیه مبتنی بر توزیع برنولی کاملاً مشهود و البته واقع بینانه تر است.

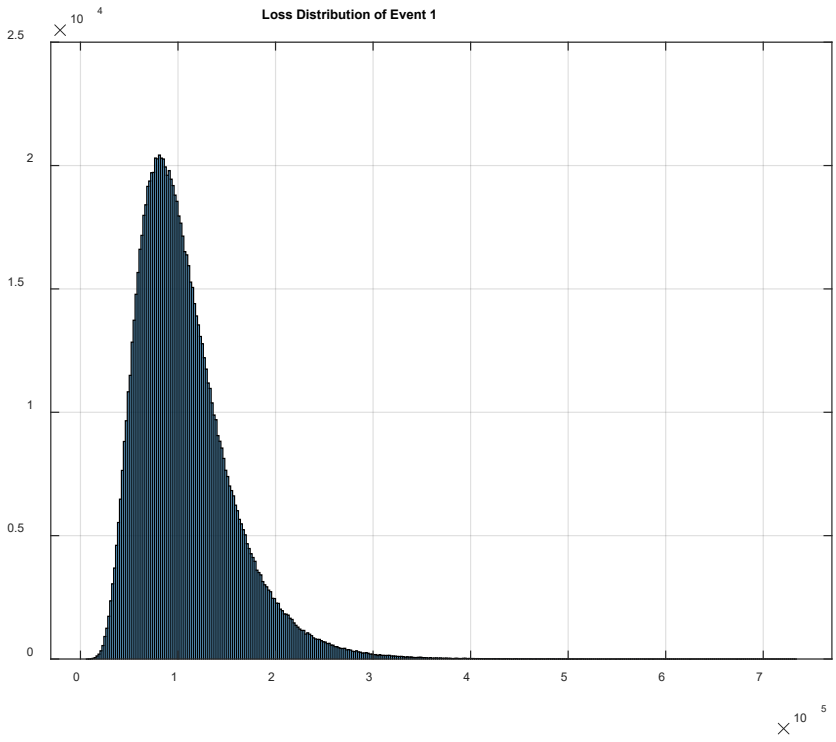
---

[1] - Iteration
[2] - Poisson
[3] - Thomopoulos 2017,p.122

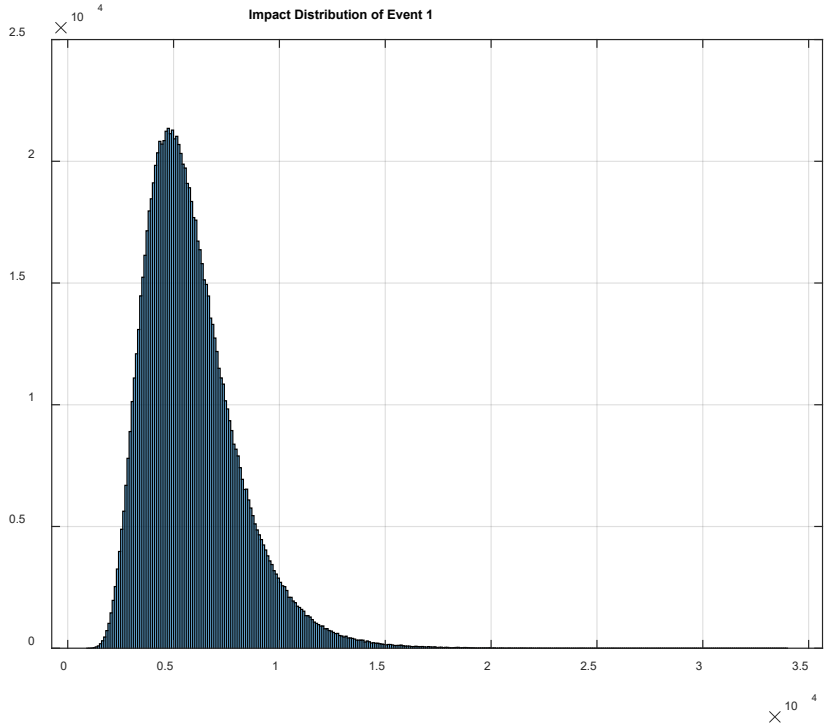
شکل ۱۱- کد برنامه شبیه سازی توزیع ضرر وقوع پدیده Event 1 با فرض توزیع وقوع پواسن و توزیع پیامد لُگ نرمال

```
clear;
clc;
m=1000000;
Impact_LB=3000;
Impact_UB=10000;
p=0.05;
lamda=p*365;
Impact_mean=(log(Impact_UB)+log(Impact_LB))/2;
Impact_std=(log(Impact_UB)-log(Impact_LB))/3.29;
A=Impact_mean*ones(m,1);
B=Impact_std*ones(m,1);
C=lamda*ones(m,1);
Impact=random('Lognormal',A,B);
Incident=random('Poisson',C);
Loss=Impact.*Incident;
figure(1)
histogram(Loss)
title('Loss Distribution of Event 1 ')
grid on
figure(2)
histogram(Impact)
title('Impact Distribution of Event 1 ')
grid on
figure(3)
histogram(Incident)
title('Incident Distribution of Event 1 ')
grid on
```

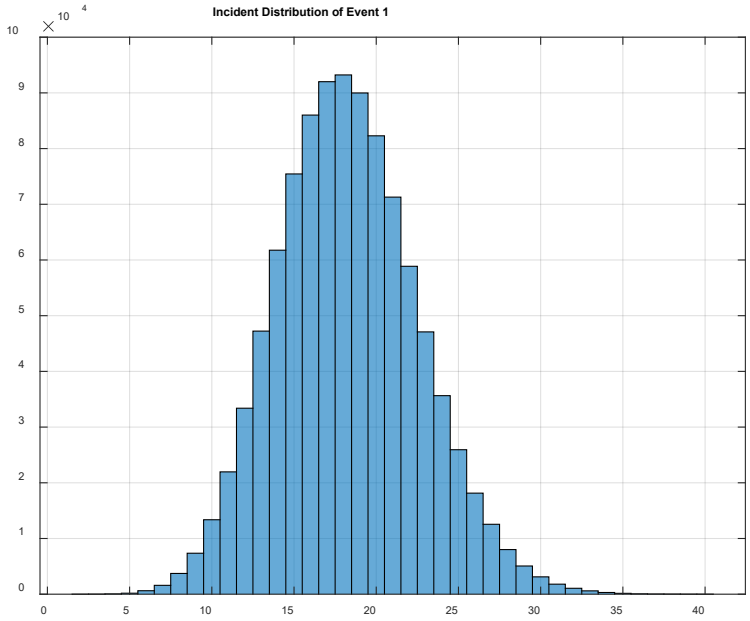
شکل ۱۱- توزیع ضرر وقوع پدیده Event 1 با فرض توزیع وقوع پواسن و توزیع پیامد لُگ نرمال



شکل ۱۲- توزیع پیامد وقوع Event 1 با فرض توزیع لُگ نرمال



شکل ۱۳- توزیع وقوع Event 1 با فرض توزیع پواسن با نرخ وقوع ثابت



۹-۴. شبیه سازی ضرر با فرض وقوع با توزیع پواسن با نرخ وقوع تصادفی λ(توزیع پواسن آمیخته نرمال)[1]

البته همانطوری که قبلاً نیز اشاره شد پارامتر p نیز بر اساس مشاهده تعداد رخدادهای نامطلوب در طی یک سال (۳۶۵ روز) به تعداد کل حالات بدست آمده است لذا بستگی مستقیم به مشاهدات تاریخی دارد و بالقوه می تواند یک متغیر تصادفی فرض شود. برهمین اساس این مقدار ذاتاً برآوردی است و از یک سال به سال دیگر می تواند تغییرنماید. از این رو به منظور واقع بینانه ترکردن شبیه سازی می توان به طور تصادفی مقدار پارامتر p را در یک بازه اطمینان ۹۰٪ انتخاب و محاسبات فوق الذکر را برای هر تکرارانجام داد. قبل از این ابتدا لازم است که بر اساس مبانی آماری این بازه را تعیین نماییم.

بازه اطمینان ۹۰٪ برای نرخ وقوع رخداد بر اساس مقدار برآورد شده $\hat{p}$

$$\hat{p} - 1.6449 \times \sqrt{\frac{\hat{p}(1-\hat{p})}{n}} \leq p \leq \hat{p} + 1.6449 \times \sqrt{\frac{\hat{p}(1-\hat{p})}{n}}$$

حال چون مقدار برآوردشده ۰.۰۵ بوده و با فرض $n = 365$ می توان بازه اطمینان را به شرح زیر برآورد نماییم:

$$0.05 - 0.0189 \leq p \leq 0.05 + 0.0189$$
$$0.0311 \leq p \leq 0.0689$$

با توجه به محاسبات فوق و مبتنی بر مبانی آمار ریاضی نتایج زیر حاصل می شود:

۱- مقدار p با اطمینان ۹۰٪ بین دو مقدار ۰.۰۶۸۸ و ۰.۰۳۱۲ قراردارد

۲- توزیع p نرمال با میانگین ۰.۰۵ و انحراف معیار ۰.۰۱۱۵ ($\sqrt{\frac{\hat{p}(1-\hat{p})}{n}}$) است. بر این اساس داریم : $Z_{0.95} = 0.0688$ و $Z_{0.05} = 0.0312$.

۳- با توجه به اینکه توزیع یکنواخت توزیع عکس هر توزیع آماری است لذا با تولید اعداد تصادفی بین دو مقدار ۱ و ۰ اعداد تصادفی با توزیع نرمال $\sigma = \sqrt{\frac{\hat{p}(1-\hat{p})}{n}}$ و $\mu = 0.05$ تولید می شود که با توجه به بند ۱ مقدار آن با احتمال ۹۰٪ بین دو مقدار ۰.۰۶۸۸ و ۰.۰۳۱۲ خواهد بود.

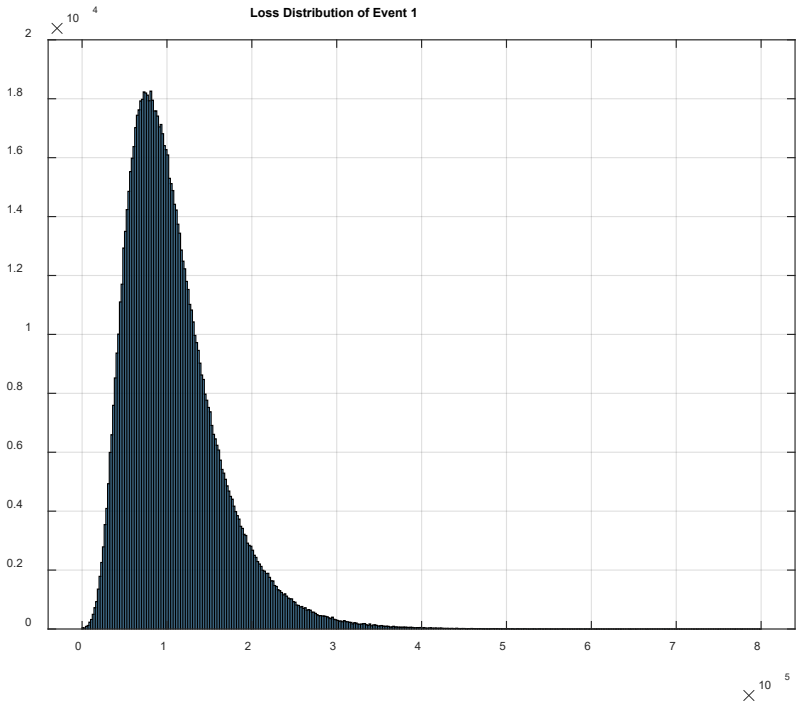
توزیع پواسن که ناشی از نرخ وقوع تصادفی باشد توزیع پواسن آمیخته نامیده می شود و بر اساس توزیع تصادفی نرخ وقوع λ تعریف می شود. در این مدل با توجه به اینکه توزیع تصادفی نرخ وقوع نرمال، توزیع پواسن آمیخته نرمال نامیده می شود. البته لازم به توضیح است که در محاسبات فوق فرض بر این بود که میانگین وقوع در ابتدا بر اساس مشاهده تعداد وقوع رخداد Event1 به کل مشاهدات محاسبه شده ولی نرخ وقوع ذاتاً تصادفی است و

[1] -Mixed Poisson-Normal Distribution

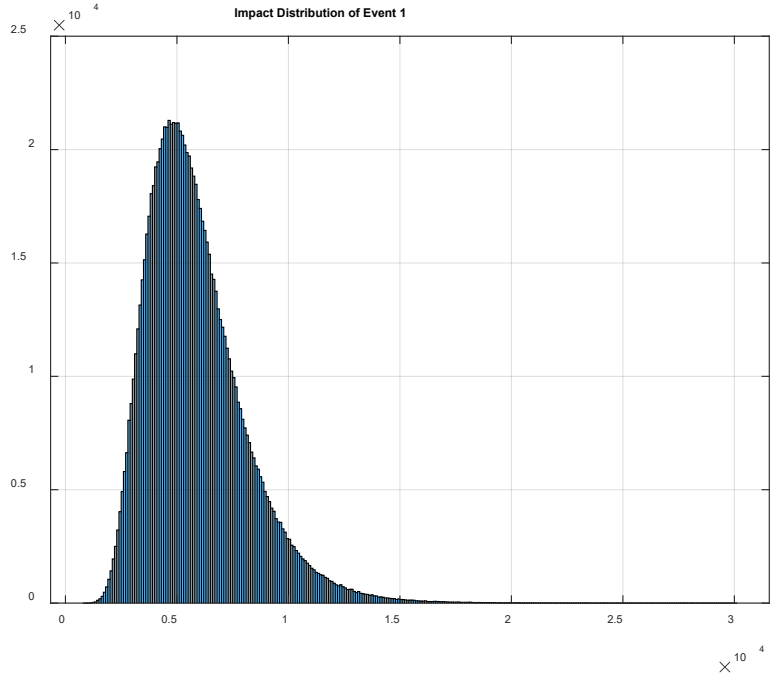
لذا بازه فوق الذکر برای برآورد آن با سطح اطمینان ۹۰٪ و بر اساس توزیع حدی نرمال تعیین شده است. لیکن عملاً در توزیع نرمال مقادیر می تواند منفی باشد لیکن احتمال وقوع اعداد کوچکتر از صفر بسیار بسیار کم است. بر این اساس کد برنامه MATLAB که تغییر یافته و هیستوگرام های مربوطه نیز در ادامه ارائه می شود. همانطوری که در نمودارها مشهود است به غیر نمودارتوزیع پیامد که عملاً تغییری ننموده است سایر نمودارها نشان دهنده کشیدگی بیشتر درتوزیع آماری مربوطه هستندکه به معنای افزایش میزان ریسک(زیان) پیامد مورد نظر می باشد.

```
clear;
clc;
m=1000000;
Impact_LB=3000;
Impact_UB=10000;
nn=365;
p=0.05;
CI=0.90;
alpha=1-(1-CI)/2;
Zalpha=norminv(alpha);
sigma=(p*(1-p)/nn)^0.5;
pUB=p+Zalpha*sigma;
pLB=p-Zalpha*sigma;
% uniarand=random('Uniform',(1-alpha)*ones(m,1),alpha*ones(m,1));
prand=random('Normal',p*ones(m,1),sigma*ones(m,1));
lamda=prand*nn;
Impact_mean=(log(Impact_UB)+log(Impact_LB))/2;
Impact_std=(log(Impact_UB)-log(Impact_LB))/3.29;
A=Impact_mean*ones(m,1);
B=Impact_std*ones(m,1);
Impact=random('Lognormal',A,B);
Incident=random('Poisson',lamda);
Loss=Impact.*Incident;
figure(1)
histogram(Loss)
title('Loss Distribution of Event 1 ')
grid on
figure(2)
histogram(Impact)
title('Impact Distribution of Event 1 ')
grid on
figure(3)
histogram(Incident)
title('Incident Distribution of Event 1 ')
grid on
figure(4)
histogram(prand)
title(' Distribution of p')
grid on
figure(5)
histogram(lamda)
title(' Distribution of lamda')
grid on
```

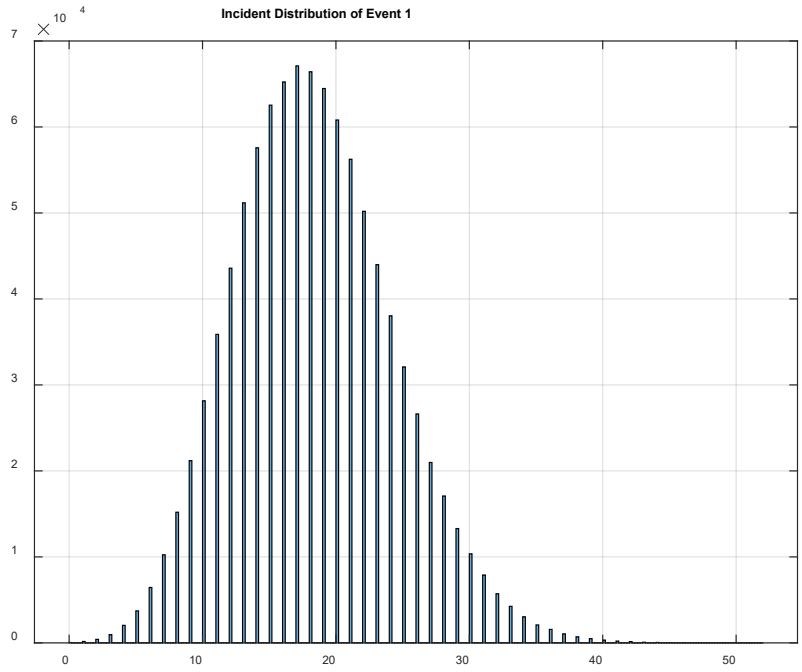
شکل ۱۴- توزیع ضرر وقوع پدیده Event 1 با فرض توزیع وقوع پواسن آمیخته نرمال و توزیع پیامد لُگ نرمال



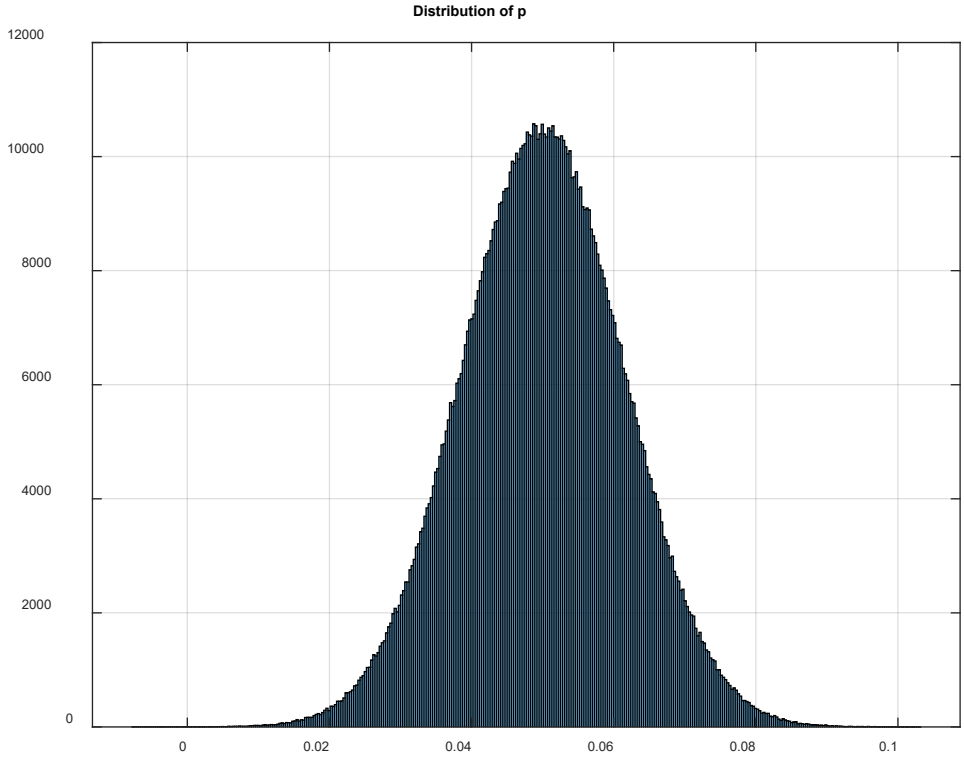
شکل ۱۵- توزیع پیامد وقوع Event 1 با فرض توزیع لُگ نرمال



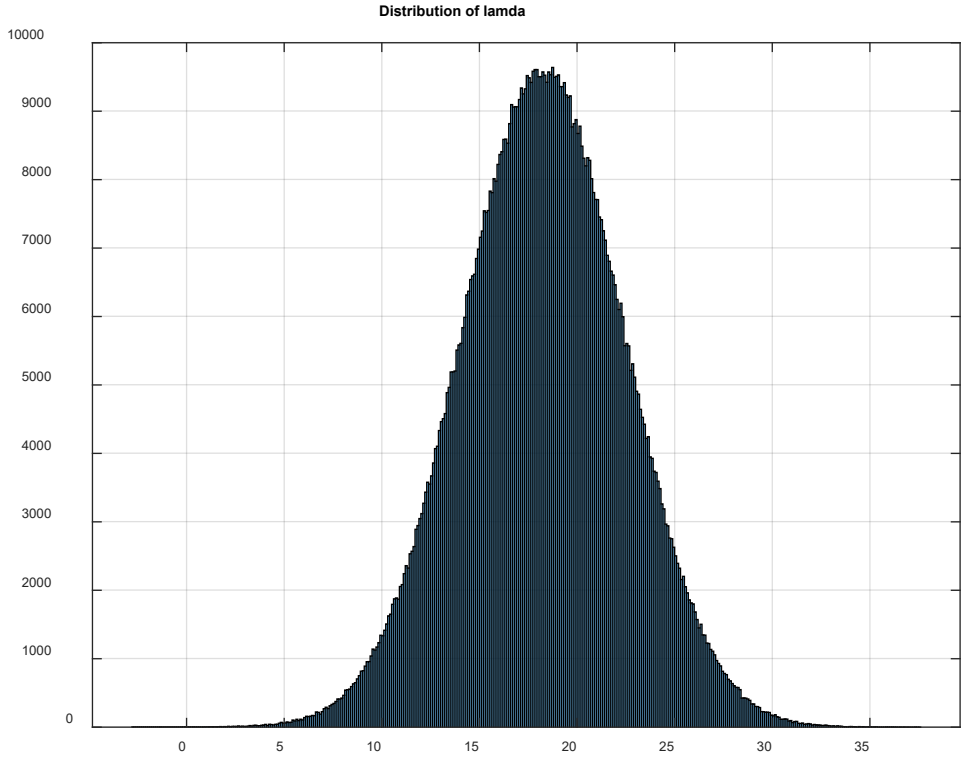
شکل ۱۶- توزیع وقوع Event 1 با فرض توزیع پواسن با نرخ وقوع تصادفی با توزیع نرمال



شکل ۱۷- توزیع نرخ وقوع Event 1 با فرض توزیع نرمال



شکل ۱۸- توزیع نرخ وقوع پواسن رخداد Event 1 با فرض توزیع توزیع نرمال



۱۰-۴. شبیه سازی ضرر با فرض وقوع با توزیع پواسن با نرخ وقوع تصادفی λ(توزیع پواسن آمیخته بتا)[1]

رویکرد محاسبه نرخ وقوع تصادفی که در قسمت قبل بیان شد مبتنی بر برآورد مقدار تصادفی این نرخ بر اساس توزیع نرمال بود و با تقریب خوبی می توانست اعداد تصادفی مثبت بین ۰ و ۱ را تولید نماید لیکن توزیع نرمال ذاتاً اعداد منفی را نیز در بر می گیرد هر چند در شبیه سازی انجام شده احتمال تولید اعداد منفی کمتر از ۰/۰۰۰۰۴٪ است که بسیار بسیار کم است و عملاً قابل چشم پوشی است. با این حال برای برآورد نرخ وقوع که عددی بین ۰ و ۱ است عملاً باید توزیعی را بکار برد که ذاتاً مقادیر بازه مزبور را در برگیرد و به توان بر اساس مشاهده تعداد وقوع که یک فرآیند تصادفی است نسبت وقوع را برآورد نمود. این توزیع بتا[2] نام دارد که در ادامه به نحوه کاربرد آن می پردازیم.

[1] -Mixed Poisson-Normal Distribution

[2] - Beta Distribution

۴-۱۱. توزیع بتا

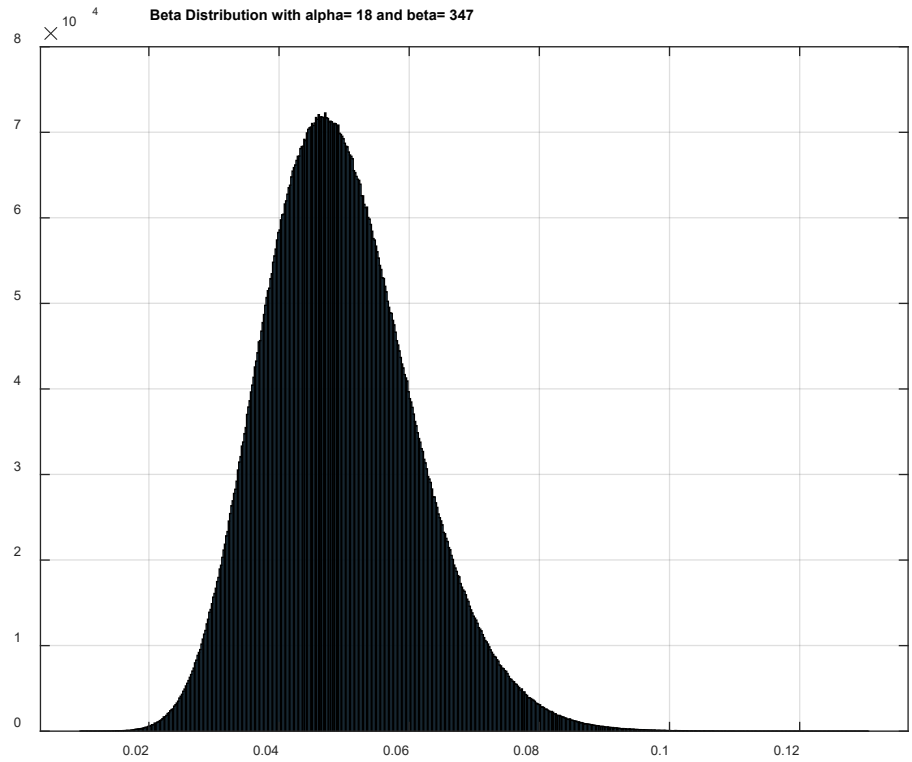
فرض کنید که در یک جعبه تعدادی گلوله سفید(پیامد مطلوب) و گلوله سیاه(پیامد نامطلوب) وجود دارد و هیچ اطلاعی از تعداد گلوله های سفید و سیاه و یا نسبت گلوله های سیاه به سفید نداریم و می خواهیم از طریق مشاهده این نسبت را برآورد نماییم(البته عملاً شمارش کل گلوله ها نیز برای ما ممکن نیست). بدیهی است قبل از هر آزمایشی با عدم قطعیت کامل برای تعیین نسبت گلوله های سیاه به سفید روبرو هستیم. برای برآورد نسبت گلوله های سیاه به سفید تعداد n مهره را از جعبه خارج می نماییم. فرض می کنیم از تعداد n گلوله ای درآورده شده از جعبه تعداد n_b مهره سیاه و n_w مهره سفید باشند در این صورت نسبت گلوله های سیاه به سفید از رابطه زیر محاسبه می شود :

$$\hat{p} = \frac{n_b}{n_w}$$

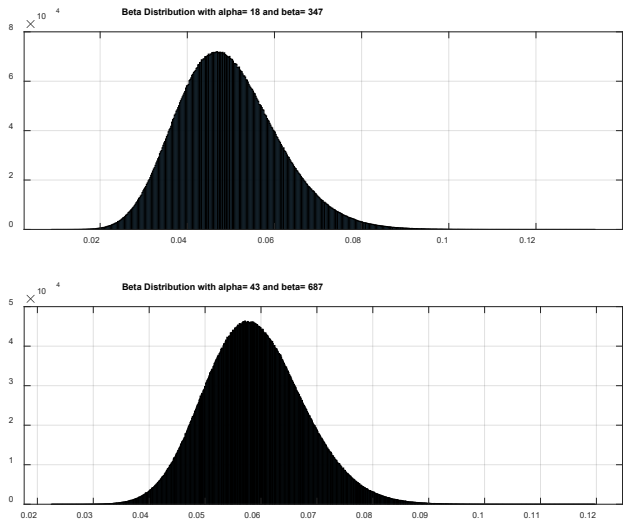
مقدار بدست آمده فوق یک برآورد از مقدار واقعی p است که در پی یافتن آن از طریق مشاهده هستیم و چون امکان تکرار این آزمایش به تعداد نامتناهی وجود دارد لذا $\hat{p}$ یک متغیر تصادفی است که مقدار آن بین صفر و یک قراردارد. توزیع تصادفی پیوسته ای که می تواند این فرآیند را توضیح دهد توزیع بتا است. بر این اساس اگر فرض کنیم که می خواهیم با یک بار آزمایش مشاهده n_b گلوله سیاه و n_w گلوله سفید حدس بزنیم که نسبت گلوله های سیاه به سفید موجود در جعبه چقدر است. توزیع بتا با دو پارامتر $\alpha = n_b$ و $\beta = n_w$ می تواند حالات محتمل برای نسبت مورد نظر را بیان کند. بر این اساس به نحوی که در ادامه آورده می شود می توان از توزیع بتا برای مدل سازی نسبت وقوع رخداد Event1 و استفاده از آن در شبیه سازی مونت کارلو سود جست.

بنابر فرض مسئله مشاهدات یک دوره یکساله(۳۶۵ روز یا ۳۶۵ مشاهده) نشان داده تعداد ۱۸ روز Event1 رخداده است و تعداد ۳۴۷ روز این رخداد مشاهده نشده است. در این صورت با توزیع بتا با پارامتر های $\alpha = 18$ و $\beta = 347$ می توان نسبت وقوع رخداد مزبور را شبیه سازی کرد. برای این منظور از کد برنامه MATLAB به شرح زیر که شبیه سازی را برای ۱۰ میلیون تکرار انجام می دهد استفاده می نماییم. جالب توجه است که میانگین این توزیع از رابطه زیر محاسبه می شود :

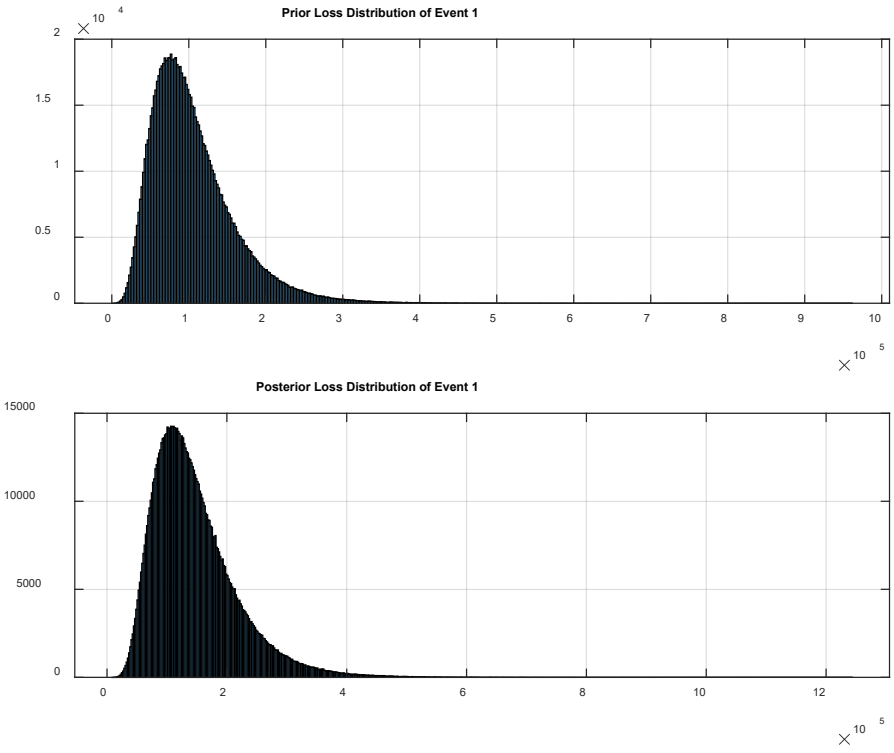
$$\mu = \frac{\alpha}{\alpha + \beta}$$

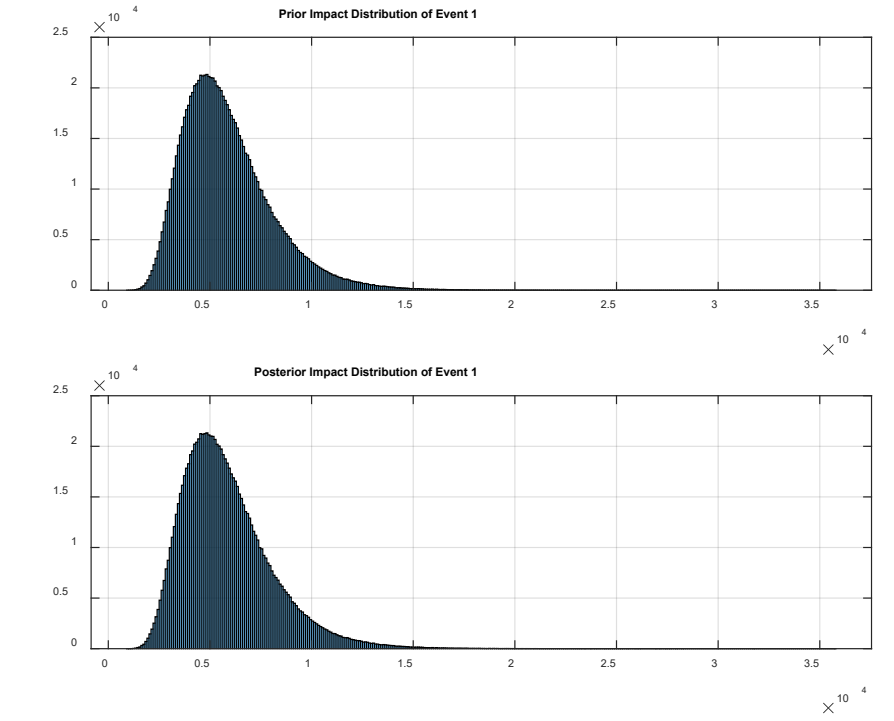


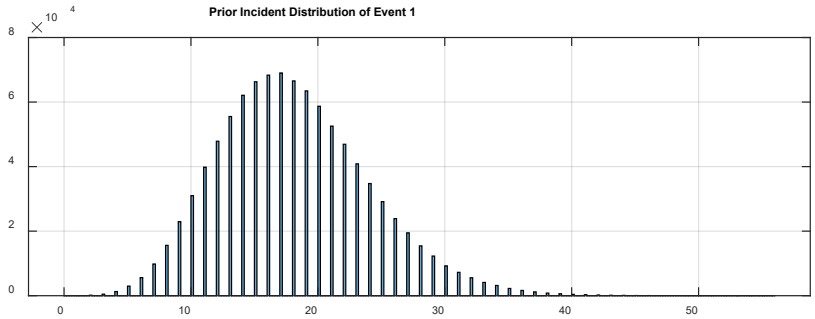
خصوصیت بسیار مطلوب توزیع بتا این است که امکان بروز شدن بر اساس مشاهدات جدید را داراست. بر این اساس می توان نگرش بیزی را نیز برای این منظور بکار برد. بدین ترتیب که اگر در اولین مشاهده به طور مثال ۱۸ حالت نامطلوب ۳۴۷ حالت مطلوب داشته باشیم و در مشاهده دوم این مقدار به ترتیب ۲۵ حالت و ۳۴۰ حالت باشد در این صورت $\alpha = 18 + 25 = 43$ و $\beta = 347 + 340 = 687$. در این ارتباط توزیع های پیشین و پسین که با ۱۰ میلیون بار شبیه سازی شده اند در نمودار مقایسه ای زیر مشاهده می شود.

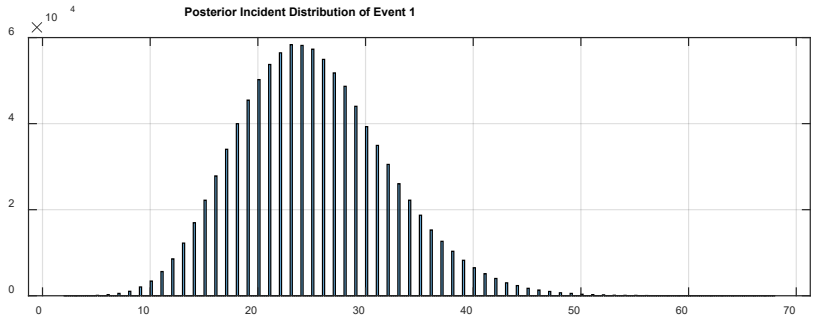


با مقدمه فوق شبیه سازی تابع توزیع ضرر بر اساس توزیع پواسن آمیخته بتا و بر اساس دو مشاهده اولیه و ثانویه صورت پذیرفت که نتایج مقایسه ای آن در ادامه آورده می شود.









همانطوری که از نمودارها مشخص است توزیع های پسین بغیر از توزیع پیامد وقوع، تفاوت کاملاً مشهودی نسبت توزیع پیشین دارند و به طور واضحی افزایش مشاهدات نامطلوب ریسک (ضرر) پیامد مورد نظر را افزایش داده است. با توجه به مدل هایی به تفصیل بیان شد و به عنوان جمع بندی در ادامه چارچوب کلی مدل سازی توزیع ضرر یک رویداد موضوع امنیت اطلاعات و به ویژه امنیت سایبری ارائه می شود.

۱۲-۴. چارچوب کلی مدل سازی ضرر وقوع یک رویداد در امنیت اطلاعات(سایبری)

به عنوان جمع بندی مطالب ذکر شده گام های زیر برای مدل سازی ضرر وقوع رویداد معین امنیت سایبری قابل انجام است:

۱- تعیین حدود بالا و پایین پیامدهای ناشی وقوع رخداد مورد نظر با بررسی شواهد عینی و یا بر اساس نظرات کارشناسان خبره

۲- تعیین تعداد وقوع رخداد مورد نظر بر اساس مشاهدات یک دوره معین و تعیین پارامترهای α و β توزیع بتا و در صورت لزوم بروز نمودن پارامترهای مزبور بر اساس مشاهدات جدید

۳- شبیه سازی وقوع با مدل تصادفی پواسن آمیخته بتا و پیامد های آن بر اساس مدل لُگ نرمال و همچنین ضرر وقوع بر اساس برآوردهای انجام شده قبلی

۴- تعیین ارزش در معرض خطر در سطح اطمینان مشخص(معمولاً در سطح ۹۵ درصد یا ۹۹ درصد) به منظور تعیین سرمایه پشتیبان برای وقوع ضرر های غیر متقربه

۱۳-۴. گسترش مدل سازی ضرر وقوع برای مجموعه ای از رویدادها در امنیت اطلاعات(سایبری)

در این قسمت قصد داریم مدل سازی ضرر وقوع برای یک رویداد را برای رویدادهای متعدد گسترش دهیم. به واقع یک بنگاه و به ویژه یک بنگاه مالی و به طور اخص یک بانک با مجموعه ای از رویدادها در امنیت اطلاعات(سایبری) روبروست که هریک به طور جداگانه می تواند موجب ضرر و زیان شود. از این رو لازم است که ضرر وقوع پدیده های مورد نظر در قالب پورتفویی از رویدادهای نامطلوب مدل سازی شود. برای این منظور برای هر رویداد در چارچوب گامهایی که توضیح داده شد شبیه سازی می شود. سپس دو حالت کلی متصور است:

۱- رویدادها دو بدو مستقل هستند که در این توزیع ضرر نهایی مجموع توزیع ضررهای هر یک از رویدادهاست.

۲- همه رویدادها دو بدو مستقل نیستند در این صورت از رویکرد کاپولا[1] استفاده می نماییم که طی آن توزیع ضرر نهایی از ترکیب توزیع ضررها بر اساس رابطه ای مدل کاپولا تعریف می نماید ساخته می شود.

برای روشن تر شدن موضوع یک مثال فرضی را در ادامه ارائه می دهیم.

مسئله ۳: فرض کنیم که دو رویداد موضوع امنیت سایبری به شرح زیر در دست است:

رویداد ۱:

- در طی ۳۶۵ روز فعالیت ۵۰ مورد(۱ مورد در هر روز) از رویداد ۱ به وقوع پیوسته است.
- برآورد ها نشان می دهد که ضرر ناشی از وقوع رویداد ۱ با ۹۰٪ اطمینان در بازه ۳۰۰۰ تا ۱۰۰۰۰ واحد پولی قرار دارد.

رویداد ۲:

- در طی ۳۶۵ روز فعالیت ۲۰ مورد(۱ مورد در هر روز) از رویداد ۲ به وقوع پیوسته است.
- برآورد ها نشان می دهد که ضرر ناشی از وقوع رویداد ۱ با ۹۰٪ اطمینان در بازه ۶۰۰۰ تا ۲۰۰۰۰ واحد پولی قرار دارد.

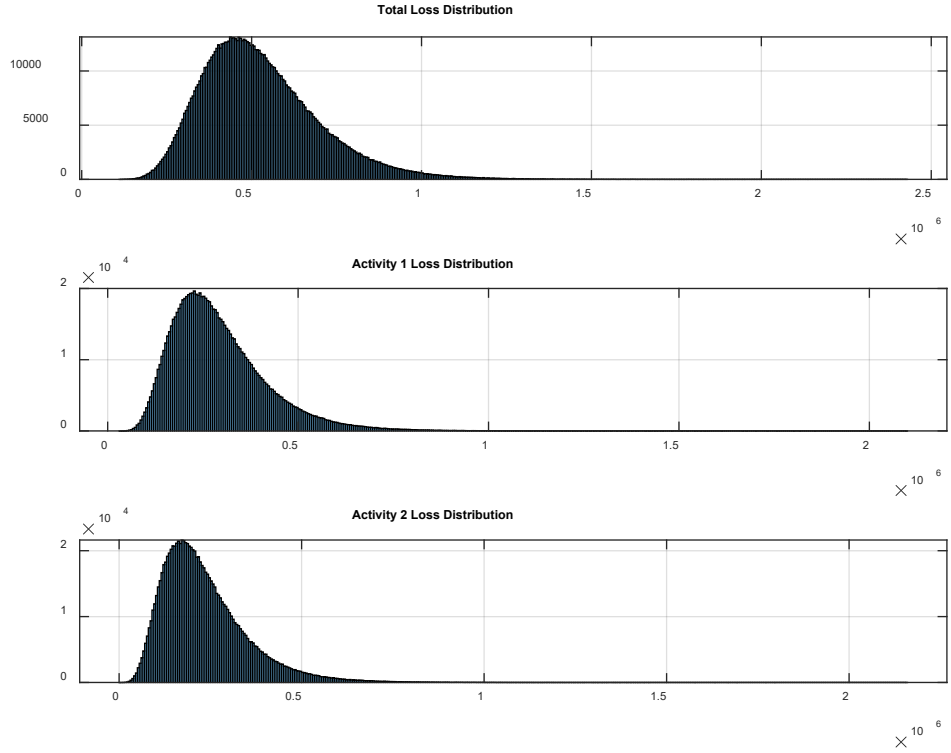
---

[1] - Capula

حال با فرض اینکه این دو رویداد عملاً مستقل از یکدیگر هستند با شبیه سازی ضرر هر یک و جمع ضرر ها با یکدیگر توزیع ضرر نهایی بدست خواهد آمد. کد برنامه MATLAB که برای همین منظور تهیه شده است در ادامه آورده می شود.

```
clear;
clc;
m=1000000;
VaR=zeros(1,2);
Impact_LB=[3000,6000];
Impact_UB=[10000,20000];
k=length(Impact_UB);
nn=365;
alpha=[50,20];
beta=nn-alpha;
Impact_mean=(log(Impact_UB)+log(Impact_LB))/2;
    Impact_std=(log(Impact_UB)-log(Impact_LB))/3.29;
    A=Impact_mean.*ones(m,k);
    B=Impact_std.*ones(m,k);
    Impact=random('Lognormal',A,B);
    prand=random('Beta',alpha.*ones(m,k),beta.*ones(m,k));
    lamda=prand*nn;
    Incident=random('Poisson',lamda);
    Loss=Impact.*Incident;
    TotaLoss=sum(Loss,2);
    figure(1)
    subplot(3,1,1)
    histogram(TotaLoss)
    title('Total Loss Distribution')
    grid on
    for j=1:2
        VaR(1,j)=quantile(Loss(:,j),0.99);
     disp(['VaR of Event ',num2str(j), 'Loss Distribution is ',num2str(VaR(1,j))])
    subplot(3,1,j+1)
    histogram(Loss(:,j))
    title(['Activity ',num2str(j),' Loss Distribution'])
    grid on
    end
    disp(['VaR of Total Loss Distribution is ',num2str(quantile(TotaLoss,0.99))]);
```

توزیع ضرر هریک از رویدادها و همچنین توزیع ضرر کل در نمودار زیر نمایش داده شده است.



ارزش در معرض خطر هریک از رویدادها همچنین کل رویدادها نیز در خروجی MATLAB نمایش داده می شود که به شرح زیر می باشد :

VaR of Event 1 Loss Distribution is 699576.8927
VaR of Event 2 Loss Distribution is 623101.1298
VaR of Total Loss Distribution is 1049090.0872

به منظور تعیین ملاکی برای مقایسه ریسک(ضرر) فعالیت های مورد بحث در ادامه شاخصی را معرفی می نماییم که در زمینه مدیریت ریسک بسیارشناخته شده وپرکاربرد است. این شاخص ارزش در معرض خطر[1] است که در ادامه تعریف می نماییم.

ارزش در معرض خطر:

هرچند مفهوم ارزش در معرض خطر در محاسبات ریسک بازار به ویژه سرمایه پشتیبان ضرر های محتمل در ارتباط با تغییر قیمت مطرح شد لیکن این مفهوم در محاسبه سرمایه پشتیبانی در برابر ضرر محتمل سایر ریسک ها از جمله ریسک اعتباری مورد استفاده قرار گرفت. بر این اساس ارزش در معرض خطر حداکثر ضرر محتمل در سطح اطمینان مشخص که معمولاً ۹۹٪ است تعریف می شود. لذا از این شاخص در ارتباط با هر توزیعی ضرری می توان استفاده نمود. به ویژه اینکه توزیع های ضرر بر اساس ارزش در معرض خطر قابل مقایسه می شوند. بدین ترتیب که توزیع ضرر با ارزش در معرض بیشتر ریسکی تر از توزیع دیگر است.

[1]- Value at Risk

۱. Publication bibliography

Antonucci, Domenic (2017): The cyber risk handbook. Creating andmeasuring effective cybersecurity capabilities. Hoboken, New Jersey: John Wiley & Sons, Inc.

Calder, Alan; Watkins, Steve (2019): Information Security Risk Management for ISO 27001/ISO 27002, Third Edition. 3rd ed. Ely, Ann Arbor, Michigan: IT Governance Ltd; ProQuest.

Hernandez, Steven; Schou, Corey (2014): Information Assurance Handbook. Effective Computer Security and Risk Management Strategies. [S.l.]: McGraw-Hill.

Hubbard, Douglas W. (2014): How to Measure Anything. Finding the Value of Intangibles in Business. 3., Auflage. New York, NY: John Wiley & Sons.

Hubbard, Douglas W.; Seiersen, Richard (2016): How to measure anything in cybersecurity risk. Online-Ausg. Hoboken, New Jersey: John Wiley & Sons.

Rohmeyer, Paul (2019): Financial Cybersecurity Risk Management. 1st ed. [Place of publication not identified]: Apress.

Thomopoulos, Nick T. (2017): Statistical Distributions. Applications and Parameter Estimates. 1st edition 2017. Cham: Springer International Publishing.