JOINT RISK MANAGEMENT SECTION

Published by CAS Canadian Institute of Actuaries Institut canadien des actuaires SOCIETY OF ACTUARIES

RISK MANAGEMENT

JULY 2020

A Pandemic Scenario: The Ultimate Systemic Risk?

By Florian Richard

Exactly a year ago, the *Risk Management* newsletter kicked off with a thought-provoking article from former Joint Risk Management Section (JRMS) Council Chair Mario DiCaro that focused on the possibility that **risks can fall through the cracks** if there isn't a clear plan on how to handle the intersecting zones of risk responsibilities within an organization. The analogy he had used was one where two volleyball players playing on the same team next to each other are responsible for their own area of the court, until the incoming ball is about to land exactly on the edge of their two areas. In the absence of a clear strategy, the ball inevitably touches the ground, handing the point to the opposing team.

Most types of insurance underwriting risks seem to fall within obvious broader risk categories—natural catastrophes, credit scenarios, human-caused events—because, despite being systemic in nature, they impact either one main product line **or** multiple product lines that are correlated to some extent.

However, which zone of risk responsibility should be in charge of pandemic risk, where a scenario can span across most existing lines of business, whether directly or indirectly?

Even before COVID-19 started changing our lives at the beginning of the year, pandemic risk was already on the radar of most property and casualty and life insurance companies. This is mainly because a handful of major local epidemics had already developed around the world over the past decade. Each one of these local epidemics taught us something different: the possibility of major event cancellation due to Zika, the severe contagion and death rates of Ebola, the short-term disruption of basic supply chains during SARS. … Projecting these types of scenarios on a global scale already had the semblance of what could be considered the **ultimate systemic risk.**

The past few months have only reinforced this preliminary impression. We have discovered that the impact is not only on claims but also on future premium. While life insurance and health insurance would seem to be the obvious product lines to be affected, most industry news seems to actually focus on event cancellation, contingent business interruption and worker's compensation. State governments have suddenly become key players in conversations around property coverage.

Short of an end-of-the-world type of scenario, is there another example of a risk with this type of reach?

Companies do their best to set up a comprehensive risk framework where risk responsibilities are clear and communicated throughout the organization. This allows enterprise risk management departments to make sure that all sources of exposure that can potentially be impacted by that risk are reported in a timely manner for aggregation purposes. Managing pandemic risk requires a coordinated effort across **all** risk functions and **all** product lines. In fact, it could be argued that it requires its own framework and governance within an organization.

I am curious to hear more from our JRMS members regarding their experience assessing pandemic risk, both before and after COVID-19. In the coming days, you will all be receiving an email that will invite you to complete a survey that looks precisely into this—across several life and property and casualty lines of business.

We look forward to your input and to sharing the results of the surveys in the December newsletter. ■

Florian Richard, FCAS, is in charge of risk management at AXA XL Reinsurance. He can be reached at *florian.richard@axaxl.com*.

September 15–17, 2020

Online Event

Jointly Sponsored by:

CAS
Expertise. Insight. Solutions.®

American Academy of Actuaries
Objective. Independent. Effective.™

CASUALTY · LOSS · RESERVE · SEMINAR

C · L · R · S

REGISTER TODAY!
casact.org/clrs

JOINT RISK MANAGEMENT SECTION

Published by CAS, Canadian Institute of Actuaries / Institut canadien des actuaires, SOCIETY OF ACTUARIES

RISK MANAGEMENT

JULY 2020

Model Governance Framework: The Basics

By Tricia Matson, Ruth Zea and Amy Alves

Editor's note: "Model Governance Framework: The Basics" by Tricia Matson, Ruth Zea and Amy Alves is an excellent starting point for any risk practitioner who is either setting up a new framework or about to reassess an existing framework. In addition to addressing all aspects of the cycle of a model, this article provides previews of ASOP No. 56, which will come into effect in October 2020 and will become the industry standard going forward.

Readers who want to learn more on this topic are encouraged to listen to the recording of the Model Governance session from Tricia Matson at the 2020 Enterprise Risk Management Symposium, where she expands on the concepts presented in this article and then applies them to case studies.

There is widespread use of sophisticated mathematical, statistical and deterministic models among financial organizations. Insurance companies use quantitative techniques and models for a variety of reasons: setting business strategy, managing risk, calculating regulatory capital, monitoring and setting internal limits, calculating exposures, pricing different products, performing stress testing and more. The use of models in the decision-making process exposes these institutions to undesirable model risk.

Standards for modeling in the insurance industry gained more attention in the late 1990s to address the role of catastrophe modeling for hurricanes and earthquakes. Since then the number and importance of modeling applications in the insurance industry has increased dramatically. After the last financial crisis, there has been increasing regulatory pressure over the appropriateness of models among financial institutions. Regulators are questioning the assumptions and limitations of models, the quality of the data used for their calibration and the thoroughness and independence of the model validation process. Regulators have been highlighting the importance of adopting an enterprise model governance framework to address risk throughout a model's life cycle.

Regulators expect senior management and model users to challenge whether the model is fit for its intended use and to understand any model limitations that may impact the model's ability to meet its intended use. Model limitation considerations include, among other things, data and assumptions. Assumptions used in the models should be challenged to assess whether or not the models would be adequate in real-life situations. In particular, it should be clear to model users under what circumstances the assumptions would no longer hold.

Given the increased use and heightened focus on modeling, the Actuarial Standards Board (ASB) began working on an Actuarial Standard of Practice (ASOP) focused on modeling, with four exposure drafts released between 2013 and 2018. In December 2019, the modeling ASOP was adopted by the ASB with an Oct. 1, 2020, effective date.[1] ASOP No. 56, *Modeling*, provides

The type and degree of model risk often varies from model to model and may depend on both the model's intended purpose and the nature and complexity of the model.

guidance with respect to designing, developing, selecting, modifying, using, reviewing, or evaluating models.

MODEL DEFINITION

Prior to the adoption of the modeling ASOP, one of the key sources of guidance on model risk management came from the Board of Governors of the Federal Reserve in their Supervision and Regulation letters on model risk management:

> The term model refers to a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates.[2]

They add:

> The definition of model also covers quantitative approaches whose inputs are partially or wholly qualitative or based on expert judgment, provided that the output is quantitative in nature.

In ASOP No. 56, the ASB defines "model" as:

> A simplified representation of relationships among real world variables, entities, or events using statistical, financial, economic, mathematical, non-quantitative, or scientific concepts and equations. A model consists of three components: an information input component, which delivers data and assumptions to the model; a processing component, which transforms input into output; and a results component, which translates the output into useful business information.3

The new standard defines "model risk" as:

> The risk of adverse consequences resulting from reliance on a model that does not adequately represent that which is being modeled, or the risk of misuse or misinterpretation.

MODEL GOVERNANCE PURPOSE

Model risk should be evaluated and, if significant, mitigated with model governance and controls. The type and degree of model risk often varies from model to model and may depend on both the model's intended purpose and the nature and complexity of the model, including any limitations of the model. A formal model governance framework, including policies and procedures to manage enterprise model risk, allows for consistency in the application of model risk mitigation strategies and provides confirmation that the model is adequately controlled throughout its life cycle.

We have identified several categories of model risk:

- **Design risk.** Model flaws due to faulty logic, methodology or theoretical unsoundness.
- **Data risk.** Risk attributable to insufficient quality and/or quantity of proper data.
- **Implementation risk.** Risk resulting from translating models into a production environment and embedding the models into an organizational process. This includes numerical inaccuracies, technological issues, source code bugs etc.
- **Calibration risk.** Risk of not properly tuning the model to real-life situations faced by the enterprise.
- **Use risk.** Risk of incorrect use of the model, inaccurate interpretation of model results or limitations imposed by the context in which the model is used.

KEY ELEMENTS AND MODEL LIFE CYCLE

Ten key elements make up an effective model governance framework:

1. **Development.** Management of model risk begins in development, when the case for a new model is started. Perhaps the most important elements involved in the process are at work here, including the work from developers who lend their experience to define the model.
2. **Documentation.** Written documentation that describes every step of the process is essential for the quick and easy identification of model components and the ability to perform efficiency review and validation. It also helps to mitigate key-person risk associated with the models.
3. **Validation.** This is considered the core phase to test models and classify their solidity. Validation refers to checking the statistical methodologies used, the input/output information and the performance. From a governance perspective, important elements to be considered include the independence of validators, frequency of validation, level of validation procedures to be performed considering the model's intended purpose and complexity, and required documentation to support and evidence the validation procedures performed.
4. **Approval.** A formal model approval process is critical for a complete model governance framework. Approval is

an essential element for financial institutions, helps evidence good governance to regulators and drives individual accountability.

5. **Implementation.** During this stage, the model is deployed to production and managed by the model users. The risk here is that some basic components, such as references to origin sources, model execution codes and/or technical documents, can be lost. A central model governance framework governing the entire model life cycle is critical to manage the risk associated with hand-offs and mitigation of any key-person risk.

6. **Modification.** As models are customized and modified, incomplete or partially complete documentation becomes a common scenario. The need to have all model elements adequately documented, including specifications, limitations, inputs and outputs, is critical to the ongoing model performance monitoring.

7. **Monitoring and retirement.** Model retirement is often undervalued or underestimated compared to the other phases. However, it is crucial to monitor whether a model is still performing efficiently or is no longer applicable given the organization's current situation. The model governance framework ought to include procedures and protocol for ongoing monitoring and, as needed, model retirement.

8. **Model inventory.** A model inventory is fundamental to obtain the big picture about models currently in use, which ones are retired or unused but have the potential to be used, what are the model uses, level of model complexity and other considerations. Models can range from simple to intricate and can also vary in the role they play within an organization. Model inventories should provide a holistic view, capturing everything related to the models from a single point of view. Additionally, model categorization may help better organize the models. For example, a model's risk can be classified by its complexity and materiality in such a way that the inventory allows tracking of every object linked, including uses, purposes, properties, changes, documentation, codes and data; and also identifying every phase in the model life cycle—that is, all the elements that contribute to model risk evaluation. An effective model governance framework often requires the use of a model inventory to ensure all models are identified, tracked and subject to ongoing validations.

9. **Information sharing.** As complexity of processes increase, communication becomes an essential factor for the parties involved, especially when there is a relationship of dependency in the phases.

It is crucial to monitor whether a model is still performing efficiently or is no longer applicable given the organization's current situation.

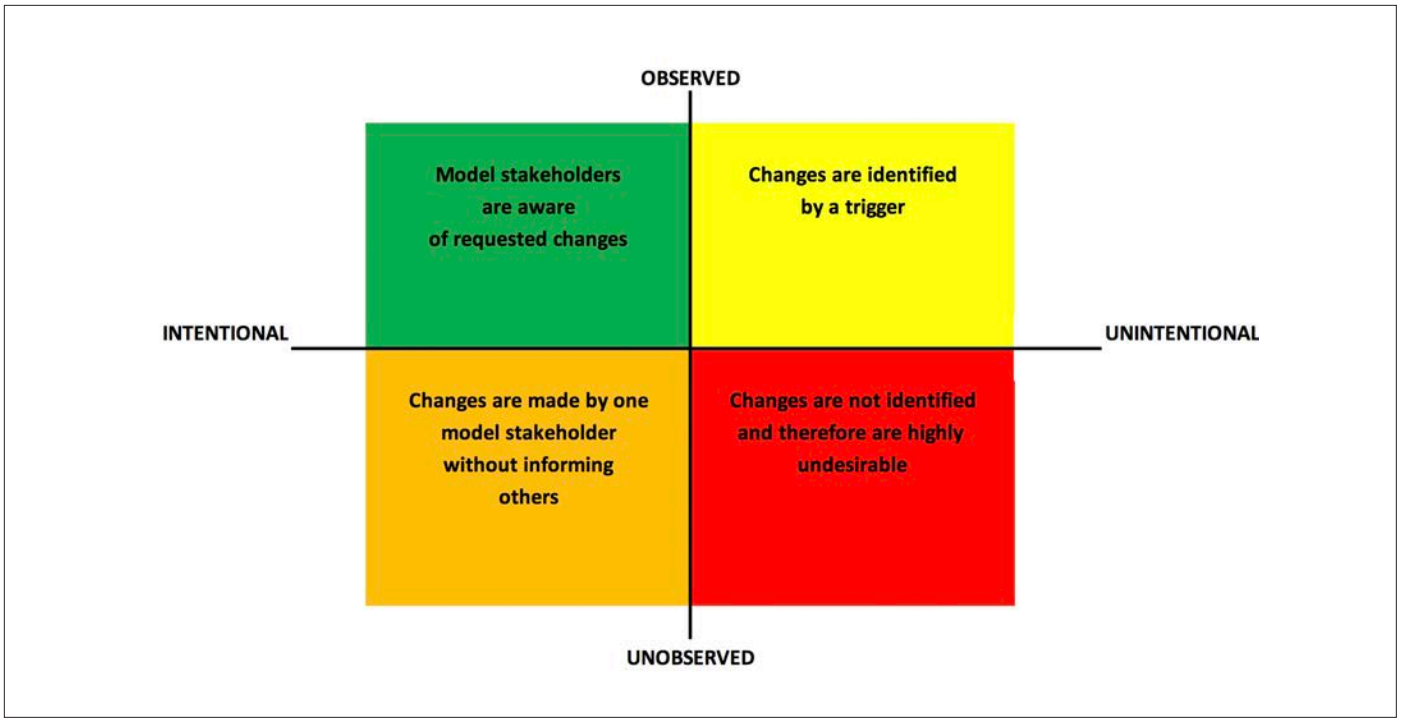
10. **Roles and responsibilities.** A governance framework ought to include a description of roles and responsibilities, allowing for better information sharing to support and govern the entire process of the model life cycle.

STAKEHOLDERS

The model governance framework often includes, as a best practice, a separate model risk management function responsible for establishing and maintaining the model governance framework, policies and controls. The model governance framework should clearly define the roles and responsibilities of the various stakeholders, including those within and external to the MRM function. Key stakeholders typically include the following people:

- **Model owner.** Party that requests and ultimately "owns" the model. The model owner sets the model's business requirements, is responsible for end-user acceptance testing and ensures a correct roll-out of the model to other users, including training, communication and other tasks.
- **Model developer.** The party responsible for the development, coding, testing, reviewing and documentation of the model, following the regulatory and business requirements.
- **Model validator**. An individual independent of the model development process, responsible for validating or testing the model.
- **Model approver.** The party charged with approving models and related model documentation prior to implementation. In some cases, this involves a committee rather than an individual.
- **Model users.** The people or teams who use the model or the model results on a day-to-day basis. Usually, the business requesting the model development, the model owner, is the main user of the model.
- **Model implementer.** Models can be implemented as stand-alone processes or within an organization's IT infra-

Figure 1
Four Types of Change in Models



structure. The model implementer is responsible for deploying the approved model for use.

MODEL RISK LINES OF DEFENSE

Model risk may occur at any stage during the life cycle of a model. Therefore, model stakeholders are part of the three-lines-of-defense principle:

- **First line.** Represented by business operations, the first line deals with model development, activity and availability.
- **Second line.** The risk management function is in charge of developing model risk management procedures and validation requirements. Model performance monitoring is typically executed within the second line in order to verify consistency, validity and efficacy.
- **Third line.** Completing the entire governance picture, the third line of defense deals with auditors, evaluating activities for effective and efficient model risk analysis and notifying deficiencies and process improvements.

MODEL CHANGES AND RISK

Models can be subject to minor or major changes at any stage during their life cycle, this is particularly true for stand-alone spreadsheet models, which are highly sensitive to changes.

In general, there are four types of change, which can be graphed on the axes of observed–unobserved and intentional–unintentional (Figure 1).

All changes can be classified in terms of impact—for example, small, medium, large and urgent.

Depending on the type and size of change, the model management process must prescribe appropriate steps to manage and mitigate the risk associated with model changes.

FINAL THOUGHTS

Managing the growing number of models, often with increasing complexity and sophistication, can be challenging and often leads to an increased level of model risk assumed by an organization. A properly designed and implemented model governance framework is essential and of foremost importance to mitigate this risk.

When establishing the appropriate model governance framework for a given organization, one ought to consider several factors.

- **Customized framework.** Model governance needs to be customized to the needs of the organization. It is not a "one size fits all" type of framework. Model governance should seek to go beyond a simple procedure, reflecting organization needs, priorities, complexities and environment.

- **Proportionality.** Costs versus benefits should be taken into consideration when investing in model risk mitigation. Assessing materiality relative to risk and economic value should drive decisions of where efforts and resources are allocated.
- **Process consistency.** In general, model governance frameworks should be consistent for all models. However, there may be cases where models with low materiality or risk potential may be subject to more relaxed requirements.
- **Pragmatic framework.** The goal of the model governance framework is to manage model risk. It should be kept as clear and simple as possible, without introducing additional risks.

As we noted, the use of models in the decision-making process exposes organizations to undesirable model risk. However, a good model governance framework can significantly lower that risk, allowing businesses to focus on what the models tell them. ■

Tricia Matson, FSA, MAAA, is a partner at Risk & Regulatory Consulting, LLC. She can be reached at *tricia.matson@riskreg.com*.

Ruth Zea, FCAS, MAAA, can be reached at *ruthzea.451@hotmail.com*.

Amy Alves, CPA, MCM, is a senior manager at Risk & Regulatory Consulting, LLC. She can be reached at *amy.alves@riskreg.com*.

ENDNOTES

1 For the final approved standard see Actuarial Standards Board, *Actuarial Standard of Practice* No. 56, December 2019, *http://www.actuarialstandardsboard.org/wp-content/uploads/2020/01/asop056_195.pdf* (accessed June 26, 2020).

2 SR 11-7: *Guidance on Model Risk Management, Board of Governors of the Federal Reserve System*, April 4, 2011, *https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm* (accessed July 1, 2020).

3 Actuarial Standards Board, *Actuarial Standard of Practice* No. 56, December 2019, *http://www.actuarialstandardsboard.org/wp-content/uploads/2020/01/asop056_195.pdf* (accessed June 26, 2020).

JOINT RISK MANAGEMENT SECTION

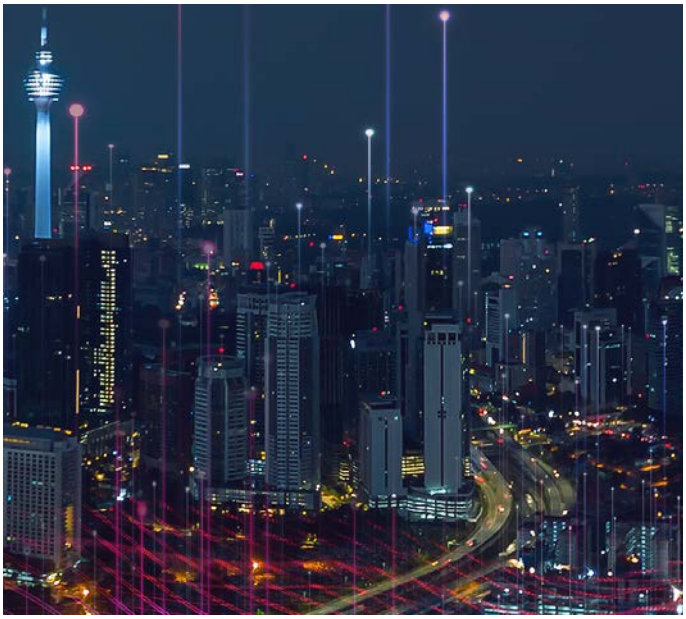
Published by

RISK MANAGEMENT

JULY 2020

Cyber: Navigating the War Exclusion Issue

By Chris Harner, Chris Beck and Blake Fleisher



Editor's note: In the ever-growing cyber insurance market, policy language is very much the focus of discussions regularly taking place among insurance professionals. This article is a follow-up to the cyber risk panel that took place at the Society of Actuaries Annual Meeting & Exhibit in 2019.

After describing the main court cases known to the industry, the authors describe the challenges associated with defining and enforcing this clause.

As cyberattacks are increasing globally in both number and intensity, the cyber insurance market is growing. According to one analysis, the global cyber insurance market size was worth $4.3 billion in 2018 and is estimated to be valued at nearly $16.7 billion by 2024.[1] Roughly 50 percent of U.S. companies have purchased cyber insurance coverage.

Increasingly, insurers view cyber as a peril and are struggling with how to model the risk, underwrite and price policies, and determine accumulation risk. In addition to the classic challenges of obtaining rich data sets and understanding correlations, insurers need to consider the uncertainty of the enforceability of policy language; specifically, the war exclusion.

Generally speaking, there is a lack of consensus in both legal and military circles regarding the definition of war, let alone cyberwar. This is a pertinent question—in fact, it's the central theme of the ongoing Mondelez v. Zurich case in Cook County Circuit Court in Illinois.[2] The answer to this question is far from clear. War exclusion clauses have long been presented as difficult issues and are full of exceptions within the conventional, physical space. The unique attributes of cyber conflict, such as attribution, plausible deniability, burden of proof and complexity and interconnectedness, add to the ambiguity of what is considered an act of war in cyberspace. While these issues remain unresolved, our goal is to identify them so that appropriate modeling decisions can be made.

Many of the court cases that involve the war exclusion issue have narrow conclusions, making it difficult to find clear precedents. In fact, some of the arguments across cases appear to contradict each other, making it difficult to determine whether the insurer or policyholder is liable. An exhaustive review of case law is beyond the scope of this paper. Rather, to demonstrate this ambiguity, we will survey some historical cases in the physical space that have dealt with war exclusions.

CASES WHERE COURTS RULED IN FAVOR OF THE POLICYHOLDER

Airlift International Inc. v. United States

In June 1967, during the Vietnam War, an Airlift International Constellation model L-109H airplane was on a flight plan from the Philippines to Vietnam, operating under a U.S. Military Airlift Command contract. Just minutes before it was about to land, a U.S. Air Force RF-4C aircraft collided with it. While the pilot and navigator of the RF-4C ejected successfully and survived, all of those aboard the Airlift International plane died and the plane was destroyed.[3]

When it came to the ensuing insurance claims, the insurer denied coverage based on the war exclusion clause. The courts ultimately decided that the collision was due to aviation peril

that could exist outside of wartime. Thus, they held that the claim was covered by insurance.

Pan American World Airways, Inc. v. Aetna Casualty and Surety Co.

In 1970, the Popular Front for the Liberation of Palestine carried out several commercial airplane hijackings, known as the Dawson's Field hijackings. Pan Am Flight 93, a Brussels–to–New York flight, never arrived at Dawson's Field. Instead, it landed in Cairo after a brief stop to refuel in Beirut. Upon landing in Egypt on Sept. 6, 1970, the aircraft exploded almost immediately after the passengers and crew disembarked.[4]

The damages were estimated at $24.3 million. The insurers argued that the loss fell within the war exclusion clauses in the all-risk policies—specifically, that the loss was proximately caused by "capture, seizure … or any taking by any military … or usurped power," by "war … civil war, revolution, rebellion, insurrection or warlike operations," or by "riots [or] civil commotion." However, the U.S. government, which covered the war risk insurance in excess of that written by private underwriters, claimed it was due to barratry on the part of the carrier.[5] The courts found the all-risk insurers to be liable for the entire loss. Part of the reasoning for this was that in 1969, aviation insurance underwriters were devising an exclusionary clause specifically covering hijacking, and Aetna could have used this clause in writing the coverage. In not doing so, "they acted at their own peril."[6]

Holiday Inns, Inc. v. Aetna Insurance Co.

During the Lebanese Civil War, the Holiday Inn in Beirut was badly damaged in the Battle of the Hotels. When Holiday Inns Inc. sought coverage under its all-risk insurance policy, Aetna Insurance Company disclaimed coverage, citing the war exclusion clause. However, the courts ruled in Holiday Inns Inc.'s favor. The judge wrote, "The Holiday Inn was damaged by a series of factional civil 'commotions' of increasing violence. The country came close to anarchy. But the constitutional Government existed throughout, the requisite intent to overthrow it has not been proved to the exclusion of other interpretations and there was no 'war' in Lebanon between sovereign or quasi-sovereign states."[7] Because Holiday Inns Inc. paid an additional premium for "civil commotion," it was entitled to recover on that policy.

CASES WHERE COURTS RULED IN FAVOR OF THE INSURER

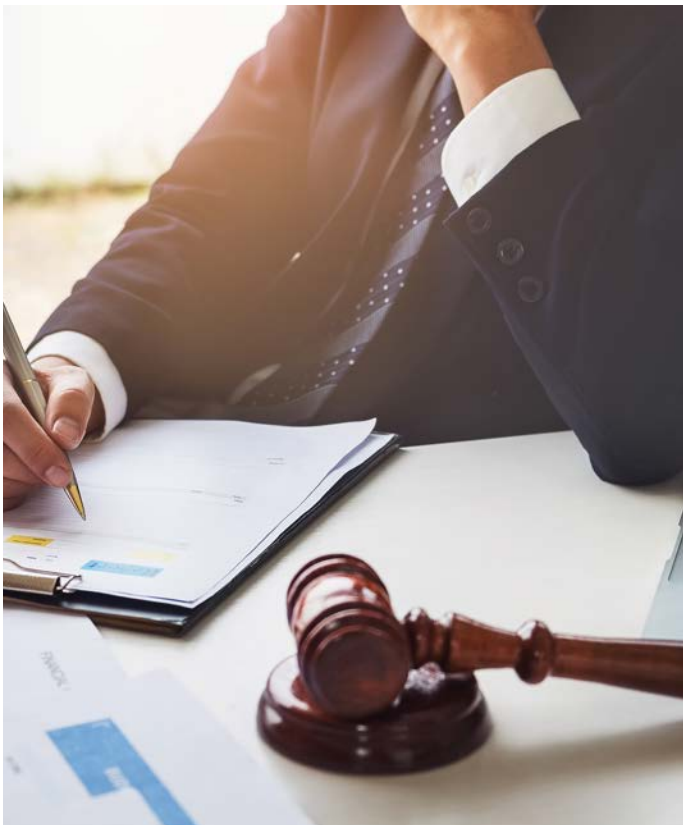
TRT/FTC Communications Inc. v. Insurance Company of State of Pennsylvania

In December 1989, Panama declared war on the United States. Panama City was in a state of civil disorder, and TRT, a telecommunications firm, operated a sales facility there. During this time, armed men dressed in plain clothes broke into TRT's Panama City facility, stealing merchandise and equipment. The insurer claimed that coverage did not apply because of the war exclusion clause. The courts determined that "regardless of whether the men were part of the Panamanian forces or a band of looters, there is ample evidence to support the conclusion that their actions against TRT were enabled by the military hostilities occurring between Panama and the United States."[8] Thus, the insurer's position was upheld.

New York Life Ins. Co. v. Bennion

On Dec. 7, 1941, Captain Bennion, the commanding officer of the USS West Virginia (BB-48), was killed when his ship was sunk at Pearl Harbor during the Japanese attack. His wife, Louise Bennion, sued the New York Life Insurance Company for the double indemnity of $10,000 due her in the event of the death of her husband by "accident." The company paid the principal sum due under the policy of $10,000. However, the policy exempted it from the liability for double indemnity. This raised the question as to whether the country was at war when Pearl Harbor was attacked or when Congress declared war the following day.

New York Life Insurance Company had no difficulty in proving that everyone regarded the attack as an act of war and, in holding for the insurance company, the court stated that it is commonly known that Pearl Harbor "commenced" the war.[9]



WAR EXCLUSIONS AND CYBER

As difficult as it is to determine whether there are grounds for a war exclusion in the physical space, it is even more challenging to make the determination in cyberspace. Part of this is due to the fact that cyber is a relatively new form of conflict, but it is also due to some of the unique features of cyber. Some of the fundamental principles of war exclusions in the physical space may still apply, such as the precedent for ambiguity in policy language. As we examined in PanAm v. Aetna, if the language in the policy is ambiguous, or if the insurer could have used language that would clearly exclude it and chose not to use that language, then the court may find coverage where it wants to. Nonetheless, even with this foundation in the physical space, there are a great deal of unknowns.

When it comes to determining whether a cyberattack constitutes an act of war, the attack on Sony comes to mind.

Sony Pictures

In 2014, North Korean hackers allegedly breached Sony Pictures as retribution for its satirical film *The Interview*. While President Obama's administration attributed the attack to North Korea, it deliberately refrained from calling the state actor attack an act of war. Instead, the administration, possibly mindful of war exclusion clauses in insurance policies, referred to the attack as an act of "cybervandalism."[10]

Sony was covered by the insurer without the war exclusion clause being an issue despite North Korea being a state actor.[11] However, not all victims of cyberattacks are so fortunate.

NotPetya

On June 27, 2017, Russia allegedly deployed the NotPetya worm through Ukrainian tax software to target Ukrainian infrastructure.[12] More detailed information on this attack can be found in the Milliman white paper *The Law of Unintended Consequences: When Companies Are Collateral Damage in a Cyberattack*.[13]

NotPetya spread rapidly and impacted businesses worldwide, including the global shipper Maersk, the pharmaceutical company Merck, and the snack food company Mondelez International, among others. These companies were not the intended targets, but rather collateral damage in a large-scale, state actor cyberattack.

Mondelez International, in particular, had numerous credentials stolen as well as 1,700 servers and 24,000 laptops destroyed. The multinational snack company owned an all-risk property insurance policy that it believed covered both the direct physical losses and the indirect expenses incurred during the period of computer failures.[14] Mondelez estimated the damage as totaling over $100 million. However, the provider, Zurich American Insurance, denied the claim, citing its war exclusion clause:

> B. This Policy excludes loss or damage directly or indirectly caused by or resulting from any of the following regardless of any other cause or event, whether or not insured under this Policy, contributing concurrently or in any other sequence to the loss:
>
> …
>
> 2) (a) hostile or warlike action in time of peace or war, including action in hindering, combating or defending against an actual, impending or expected attack by any:
>
> (i) government or sovereign power (de jure or de facto);
>
> (ii) military, naval, or air force; or
>
> (iii) agent or authority of any party specified in i or ii above.[15]

Mondelez claimed its coverage did not result from a cause or event specified in the war exclusion clause, and that Zurich wrongfully denied its coverage. According to the complaint, Zurich's senior management recognized the coverage denial was wrongful and improper, and the insurance company promised Mondelez that it would rescind its denial of coverage and ultimately agreed to a $10 million partial payment that was unconditional and not subject to a "clawback" provision.[16] However, despite Zurich rescinding its denial of coverage, Mondelez never received the funds and decided to take legal action against Zurich.

The outcome of this case will likely have profound implications for cyber insurance. If the court finds for Mondelez, then insurers may need to rethink whether they want to continue underwriting a line of business in which the courts will not enforce the war exclusion even though state actors have the greatest ability to trigger claims. They also need to rethink their underwriting language, as the ambiguity in the war exclusion clause often leads to the courts ruling in favor of policyholders. Conversely, if the court finds for Zurich, then corporations must rethink whether it makes sense to purchase insurance that will not pay out when a state actor inflicts significant harm on the business.

In addition to implications of the enforceability of the war exclusion, one of the most critical questions that courts will need to resolve is, what constitutes an act of war in cyberspace? Depending on the manner in which this question is answered, insurance providers may be unable to cite their war exclusion clauses in an effort to deny coverage. Given the history of court cases regarding "traditional" war, it appears claims may

have to be adjudicated on a case-by-case basis. Because state actors are so deeply entrenched in cyberwarfare and companies can be attacked unintentionally anywhere in the world, broad definitions for cyber acts of war could render cyber insurance useless. Alternatively, some definitions may be able to render the war exclusion clause to be essentially useless, in which case insurance payouts may be higher than the premium anticipated, causing insurance for cyber-related damages to become unprofitable.

UNIQUE FEATURES OF CYBER

Some unique features of cyber make the war exclusion issue particularly complicated. In this section, we explore three of these features: plausible deniability, burden of proof and complexity and interconnectedness.

Plausible Deniability

One of the novelties of cybercrime is that it is relatively difficult to attribute the attack to a particular party because hackers, especially state actors, are able to cover their tracks. This provides the attacker with plausible deniability, which is often a highly sought after quality in geopolitical conflicts. In a sense, plausible deniability allows state actors to pursue certain actions that may not be consistent with the current body of international law and norms. That said, although it is difficult to determine the identity of an attacker in cyberspace, it is not impossible. Nation-states and cybersecurity firms frequently use digital forensic techniques to determine the perpetrator of cyberattacks to a certain likelihood.

Burden of Proof

Although it is possible to determine the attacker to a certain degree of confidence, insurance companies still bear a burden of proof. For instance, state actor intelligence agencies are not going to get into specifics about the methodology used to attribute the attack to a particular actor. This is in part not to expose their own tools and capabilities, but also not to expose top secret intelligence or jeopardize ongoing operations. There could also be situations in which a state actor does not wish to publicly attribute the attack to a particular country if it fails to suit its national interests at the time. Furthermore, relying on the assurances of third-party companies or governments raises questions: Which companies and nation-states' declarations of attribution are valid for an insurance claim? In addition, even if the attack is attributed to a particular actor, what degree of likelihood is necessary for attribution? What kind and how much information is required? All of these questions would likely need to be resolved in some form when it comes to determining whether an insurance company can use its war exclusion clause.

Complexity and Interconnectedness

As seen with NotPetya, the interconnected nature of cyber makes it difficult to determine whether a company was the intended target. In a sense, all companies could be fair game for a state actor attack even if they do not operate near a war zone. Not only does this make it more challenging for companies to protect themselves, but it also makes it more challenging for actuaries to model the risk. In particular, there is a great deal of uncertainty in the legal system, given what appears to be the lack of a single overarching precedent. Furthermore, a company located in a remote area with very little crime could become the victim of a state actor cyberattack as collateral damage. This is very difficult to predict, but something actuaries and underwriters need to account for when assessing the risk.

CONCLUSION

The uncertainty that surrounds these legal and regulatory concerns creates additional complexity in understanding and modeling cyber risk. In particular, the issues outlined in this article highlight critical coverage issues that future pricing models will need to incorporate. Case law will likely evolve slowly regarding how the courts may view cyberattacks and their consequences. With the ambiguity in legal definitions, it is important to think through the direct and indirect consequences of a cyberattack being declared an act of war. ■

Chris Harner, FRM, is managing director of Cyber Risk Solutions at Milliman. He can be reached at *chris.harner@milliman.com*.

Chris Beck is an executive risk consultant in the Cyber Risk Solutions group at Milliman. He can be reached at *chris.beck@milliman.com*.

Blake Fleisher is a senior cyber risk analyst in the Cyber Risk Solutions group at Milliman. He can be reached at *blake.fleisher@milliman.com*.

ENDNOTES

1 Dwyer, K. Cyber Insurance Capacity Could Quadruple in Six Years; Don't Let Your Coverage Lag. *Risk & Insurance.* March 6, 2020. *https://riskandinsurance.com/commercial-cyber-insurance-could-quadruple-in-six-years-dont-let-your-coverage-lag/* (accessed May 24, 2020).

2 Mondelez International Inc. v. Zurich American Insurance Company (Circ. Ct. Cook County, Ill. 2016). *https://www.scribd.com/document/397265756/Mondelez-Zurich* (accessed May 24, 2020).

3 Airlift International, Inc. v. United States, 335 F. Supp. 442 (S.D. Fla. 1971). *https://law.justia.com/cases/federal/district-courts/FSupp/335/442/1737917/* (accessed May 24, 2020).

4 Marquard, B. Obituary: John Ferruggio, at 84; hero of 1970 Pan Am hijacking. *Boston Globe,* June 22, 2010. *http://archive.boston.com/bostonglobe/obituaries/articles/2010/06/22/john_ferruggio_of_milton_hero_of_1970_pan_am_hijacking_dies_at_84/* (accessed May 24, 2020).

5 Carrier in this context is referring to the airline carrier Pan American World Airways, Inc.

6 Evans, Alona E. 1975. Pan American World Airways, Inc. v. *The Aetna Casualty and Surety Co. Et Al. The American Journal of International Law* 69, no. 2:415–431. doi:10.2307/2200277 (accessed April 28, 2020).

7 Lewin, T. Beirut Insurance Ruling Favors Holiday Inns. *New York Time*s, Sept. 21, 1983, *https://www.nytimes.com/1983/09/21/business/beirut-insurance-ruling-favors-holiday-inns.html* (accessed May 24, 2020).

8 Caban, E.E. 2003. War-risk, Hijacking and Terrorism Exclusions in Aviation Insurance: Carrier Liability in the Wake of September 11, 2001. *Journal of Air Law and Commerce* 68, no. 2:8. *https://scholar.smu.edu/jalc/vol68/iss2/8* (accessed May 24, 2020).

9 Borchard, E. 1947. When Did the War Begin? *Columbia Law Review. https://digitalcommons.law.yale.edu/fss_papers/3413/* (accessed May 24, 2020).

10 Satariano, A., and N. Perlroth. Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong. *New York Times*, April 15, 2019, *https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html* (accessed June 5, 2020).

11 Rand, J.M. A Tale of Two Carriers: *Disparate Views of War/Terrorism Exclusion. Cyberinsurance Law Blog,* March 28, 2019, *https://www.databreachninja.com/a-tale-of-two-carriers-disparate-views-of-war-terrorism-exclusion/* (accessed May 24, 2020).

12 Greenberg, A. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*, August 22, 2018, *https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/?verso=true* (accessed May 24, 2020).

13 Harner, C., C. Beck, and B. Fleisher. The Law of Unintended Consequences: When Companies Are Collateral Damage in a Cyberattack. Milliman white paper. March 9, 2020. *https://us.milliman.com/en/insight/the-law-of-unintended-consequences-when-companies-are-collateral-damage-in-a-cyberattack* (accessed May 24, 2020).

14 Corcoran, B. What Mondelez v. Zurich May Reveal About Cyber Insurance in the Age of Digital Conflict. *Lawfare*, March 8, 2019, *https://www.lawfareblog.com/what-mondelez-v-zurich-may-reveal-about-cyber-insurance-age-digital-conflict* (accessed May 24, 2020).

15 Mondelez v. Zurich, supra note 2.

16 Ibid.