2019 Cyber, Management and Professional Liability Conference
July 10-12, 2019
Boston, MA

Torts of the Future; Evolving Trending in Cyber Claims; and Related Coverage Issues

The world of cyber claims continues to evolve with threats to insureds constantly changing. Various strains of ransomware and other forms of malware are becoming more virulent leading to more severe claims, including business interruption losses. Business email compromise (BEC), phishing and DDoS attacks continue to plague companies as well. This panel, which is comprised of cyber industry experts including a practitioner, broker and insurance carriers, will discuss the main drivers of cyber claims in 2018 and the first half of 2019. The panel will also try to look to the future to address upcoming concerns for the industry beyond what is considered the traditional cyber risk.

The panel will also discuss how cyber coverage continues to develop to meet the needs of insureds in this rapidly changing environment. We will explore how Cyber policies frequently interact with other coverages, including Tech E&O, Media, Property, EPL, CGL Crime and other insurance products.

I. Torts of the Future

Robotics and Artificial Intelligence

You can read about the use of Robotics in the news on nearly a daily basis. Robots are commonly used in warehouses and manufacturing plants today. The first reported death involving a robot in the workplace was in 1979. Robotics at that time was in its infancy and was considered prohibitively expensive. Things are rapidly changing and Robots in the workplace are becoming commonplace as countries such as Japan face an aging population and decreasing workforce. Additionally, labor costs continue to escalate and purchasing a robot for $35,000 and the maintenance required is considerably less than the costs associated with hiring human employees. Robots are moving beyond manufacturing and into the service sector. Robots are used by hotels to deliver room service, they are used in the health care industry to assist in diagnosing as well as drawing blood; and in the restaurant business they are being used to take orders, to cook and deliver food.

Robots are also used in the form of Exoskeletons. Employees are able to wear Exoskeletons to increase their physical strength while maintaining the dexterity and hand control of a human.

The use of Exoskeletons in the workplace is expanding rapidly and is limitless. Not only does the use of Exoskeletons increase human strength, they also show great promise in assisting persons with disabilities in overcoming those disabilities to open up jobs that such persons ordinarily would not have. With the limitless possibilities opens the employer to litigation in the reasonable accommodation world of the Americans with Disabilities Act. If lifting 50 pounds is considered an essential job duty, and if an Exoskeleton device exists such that any employee could lift 50 pounds, is it a reasonable accommodation to provide all employees with an Exoskeleton so everyone can lift 50 pounds? To date, there is no litigation on this subject but I anticipate it is only a matter of time until there is.

Cases involving Robots and Torts of the Future

Williams v. Litton Systems, 416 N.W.2d 7604, 164 Mich. Ap. 195 (1979):

The first reported death by Robot in the workplace was in 1979. The plaintiff in the Williams v. Litton Systems matter, Robert Williams, is considered the first human to ever be killed by a rogue robot. Williams was an operator of a parts-retrieval robot at a Ford plant that included one-ton transfer vehicles and was designed to retrieve items from a high-density storage area. On January 25, 1979, the robot appeared to malfunction and was not retrieving the parts and keeping inventory in the manner that it was programmed to do. Williams then had to manually climb the storage shelves himself and was killed when he was struck from behind by a one-ton transfer vehicle.

The manufacturer of the parts-retrieval robot, Litton Industries, was sued by the Estate of Williams who alleged that Litton Industries was "negligent in designing, manufacturing and supplying the storage system and in failing to warn the decedent of foreseeable dangers in working within the storage area." (Williams v. Litton Systems, Inc., 164 Mich. App. at *197) and in 1983, a jury found in favor of the Estate and awarded them $10,000,000. Litton Industries sought recovery of judgment costs from Ford because Ford did not "submit the decedent for training programs provided by Litton and by allowing the decedent to enter the storage system when the lockout system was off." (Williams v. Litton Systems, Inc., 164 Mich. App. at *198). However, the appellate and supreme court of Michigan dismissed Litton's claims because they already settled with the Estate.

Elsea v. Ajin USA matter Circuit Court of Chambers County, Alabama 12-cv-2016 – 900140.00:

Elsea, a contract employee, was a machine operator at Ajin USA, a South Korean-owned plant that made car parts for Hyundai and Kia. In June 2016, a robot that Elsea was overseeing began to malfunction and ceased to work. Elsea and colleagues requested assistance for someone to come and fix the robot, but when calls went unheard, they entered the caged area designed barricade the machine and Elsea's torso was crushed when the robot abruptly restarted; she died the next day.

Elsea's estate filed a lawsuit against Ajin USA, as well as Elsea's staffing agency and the manufacturers of the robot alleging, among other things, that the machine was "unreasonably dangerous and defective in that it created an unreasonable risk of serious injury or death to the intended user." https://issuu.com/lucyberrydebuty/docs/ajin

Holbruck v. Prodomax Automation LTD (US District Court WD Michican Southern Division 1:17-cv-00219

The court has not decided on the motion to dismiss FANUC Corp. (the Japanese corporation) for lack of personal jurisdiction, instead opting to allow plaintiff time for limited discovery in order to establish jurisdiction, and then allow for supplementary briefs to be filed.
The supplementary briefs were filed under seal; per the docket, and as of March 8, 2019, the court has yet to decide on the matter of jurisdiction.

In the meantime, Nachi Robotic Systems (a Delaware corporation) has filed a motion for summary judgment claiming they did not "manufacture, sell, install, design, test, service, alter, or provide anything involved in this incident." This motion is currently pending as of March 8, 2019.

Boeing 737 Max Airplane Accidents and Software Patch to address

The recent Boeng 737 Max airplane disasters are going to be interesting to follow as additional facts are revealed. On March 10, 2019 157 people died and five months earlier 189 people died. There are indications that software intended to prevent the jets from stalling may have played a role in both accidents and a software patch is already available to address the issues that may have caused the 2 crashes. The question that will be developed is whether the plane was inherently dangerous when it entered the stream of commerce and whether the software patch will truly solve the issue. This analysis is being developed in the medical device world as well. We will provide up to date information on the Boeing 737 Max and medical device patches in our presentation which have not yet been reported on.

Artificial Intelligence in hiring and in entitlement distribution

Artificial Intelligence ("AI") is widely used in hiring among most Fortune 500 companies. Amazon stopped using its AI when it realized it was inherently biased against woman. AI in hiring uses common human features such as smiling and eyebrow movements in evaluating whether an applicant will be a "good fit" or not. Scores are given to each applicant. As demonstrated by the Amazon revelation, the potential for bias exists. So far, the EEOC is taking a "wait and see" approach, but it is anticipated that change is on the horizon.

Artificial Intelligence is used by many government entities to determine who may be permitted to receive benefits. This is known as Automated Decision Making Systems. Advocates are pushing the Government to confront Machine Bias – and calls on the developers that sell products to the government agencies to release certain information like product's source code, a description of the algorithms used and a training data set to allow the public to meaningfully assess how such systems function.

There has been litigation surrounding this. in 2012, the ACLU – USDC (D Idaho) ruled that a contractor with Idaho's Medicaid Program had t o reveal the algorithm used to determine annual Medicaid funding levels. The ACLU raised a red flag after it was disclosed that htousands

of people in the state were losing their Medicaid coverage – upon examining the algorithms, ACLU found the formulas to be biased and based on incorrect data sets.

K.W. v. Armstong – (https://www.law.com/the recorder/almID/1202728529292 argued algorithms should NOT be used and District Court ultimately agreed. Arkansas has a similar case regarding automated decision making systems – in March, 2018 the Arkansas Department of Human Services had to stop using an algorithm to determine how many hours of home care to allocate disabled Medicaid recipients in the state. The ruling was in response t a lawsuit by Legal Aid Arkansas that required the state to first submit the algorithms for public comment and review by the state's legislature before going into effect.

Internet of Things

With the advent of 5G fast approaching and the number of connected devices escalating, IoT exposures are anticipated to increase exponentially. California's Iinternet of Things legislation is sure to be copied by other states and carriers need to be aware of the potential claims out there.

General overview of coverages

We will discuss the Incident Response insuring agreement on a couple different cyber policies. We will explore the concept of digital asset loss and network extortion and recent claims our panel has handled concerning the same such as wire fraud and ransomware real life scenarios. We will also talk about how the panel members have handled business interruption and contingent business interruption.

We will cover some recent privacy liability including Illinois' BIPA law and its private right of action in light of the Six Flags Decision. It is widely anticipated that the world of privacy litigation is about to explode. Wal Mart is using an AI assisted shopper, at a known "loss" in the hopes of competing against Amazon. Stores are using facial software to predict shopper's spending habits so that the shopper may be targeted with tempting items to purchase.

Claim Triggers

Real life claims for first party coverage will be covered to demonstrate when coverage will be triggered for data breaches, business email compromises and phishing. Phishing claims continue to result in big payouts for insurance carriers. Ransomware and other forms of Malware claims will be talked about and attempts to generate audience participation will be made. DDoS Attacks and trends will be addressed.

We will also talk about Third party claims that arise including privacy/data breach related actions. We will talk about standing to bring claims under statutes such as BIPA, CCPA, MVRPA. And we will talk about PCI and Regulatory matters.

Interaction with Other Policies

The pending litigation involving insurance carrier Zurich and its War Exclusion is being closely watched by the insurance world. The definition of War is about to be re-defined. Nearly every insurance policy has hidden cyber risks and its imperative that insurance professionals grasp the role technology is playing and how it effects Property, Commercial General Liability; Crime; Directors & Officers; Tech E&O; media and EPL policies. We will provide real life examples including the Urkaine power plant that is believed to have been hacked by Russia and other state actors attacking critical infrastructure worldwide.