Swiss Re

Trend Spotlight

Smart homes – their impact on insurance claims

Consumers are drawn to smart-home technology. They like the convenience of being able to remotely monitor and control climate, lighting and entertainment devices. As this technology becomes more effective and more common – and leads to fewer and smaller insurance claims – homeowners may soon be asking for discounted insurance premiums.

While much of the new smart-home technology focuses on convenience, some types of technologies will prevent or mitigate the leading perils that cause losses under homeowner's policies such as water damage, burglary or fire. Let's look at the latest smart-home technology and how it can help insurers.

What's a "smart home"?

Smart homes have electrical, security, multi-media and climate-controlled systems that can be monitored or operated remotely by a computer or on a smartphone. The features of smart systems vary significantly depending on the amount the homeowner wants to spend or build into their home. The use of technology to connect the home to the homeowner is likely to grow, and insurers can benefit if they fully understand this technology.

Water damage: the most frequent cause of loss

According to the Insurance Information Institute, in 2014, water damage claims were the most frequent type of homeowner claim. In fact, one out of three homeowner claims filed was a water damage claim.[1] Water damage claims are more frequent than fire, wind, hail, theft or any other type of peril covered under a homeowner's policy.

Automatic and remotely operated thermostats have been popular features for a few years. People have embraced the comfort of coming home to a warm home and the cost savings of running the heat and air only when needed. This technology is also very useful in preventing frozen pipes and resulting water damage losses.

Newer, more sophisticated technology is now being installed in smart homes, specifically designed to mitigate or prevent water damage claims. These systems monitor moisture levels or water usage and allow the homeowner — or the home itself — to intervene when the system detects a problem. The new technology is a more effective tool against a broader range of water claims. Generally, there are two types of systems designed to detect water leaks: sensor and flow systems.

With sensor technology, water sensors are placed where a leak is likely to form – near water heaters, washing machines, dishwashers or even attic spaces under leaky roofs. Depending on the complexity of the system, the sensors can put out an alarm, send a message to a computer or smartphone or even automatically shut off a water valve when the system detects water. The problem with these sensors is coverage. The sensors usually require some contact with actual moisture, not just

© 2016 Swiss Re

humidity, to activate an alert, and they must be placed in the right spot. The good news: these sensors can cost as little as $10 per sensor and some can be installed by anyone.

Flow technology is quite a bit more sophisticated. The system constantly measures the flow of water through the pipes and sounds an alarm or shuts off the water supply when the system detects abnormal flow or pressure. The homeowner receives a message by phone warning them of a possible leak. Flow systems usually require professional installation and can be very costly. A drawback to these systems is that they don't detect water intrusion from an outside source, such as a leak in the roof.

While a water leak system won't prevent all water damage claims, it can detect a leak quickly and the system or the homeowner can take immediate action. If a water leak is noticed immediately and dried out quickly, there will be less damage to the home than if a "gusher" of a leak goes undetected for hours or days. Sometimes even more costly than the gushers are small, slow, hidden water leaks that can lead to mold. These claims create difficult coverage issues and require special care from the claims handler. Smart-home technology can have a big impact on the frequency and severity of these losses.

Security

Burglary or vandalism are other common perils that smart homes can help eliminate or mitigate. Because of the low cost, simple installation and ease of use, home security systems are one the most accessible and popular smart-home technologies. Homeowners are installing remotely operated locks, security cameras and automatic lighting with increasing frequency. While many homes have an alarm system monitored by a central alarm company, smart homes may go beyond the central alarm system. Some have locks that open electronically through smartphones and can provide a record of who entered a home. Other systems now trigger photographs or video footage sent directly to the homeowner's smartphone. In either case, not only does the technology deter the break-in, it provides a record for the claims handler of how the loss happened, who caused the loss and even photographic evidence of what items were taken or damaged.

Smoke and fire

While water losses might be the most frequent type of homeowner loss, the most severe are fire losses, averaging around $39,000 per claim.[2] Smoke and fire alarms have been around for decades. Improved smart technology offers benefits not previously available. It's much easier to monitor these alarms remotely. If a homeowner isn't home, or in an area where they may not hear the alarm, the system can send an alert to their phone, allowing for an earlier response. New alarms have better technology to detect smoke and flames and distinguish a real fire from steam or burnt food. To prevent these false alarms, alarms were usually installed in bedrooms and hallways. Homeowners are installing this improved technology in locations where a fire is most likely to start or even in the appliances. When an alarm senses an issue in an appliance, the system can immediately shut down the electrical supply to that appliance, or at the very least, send an earlier alarm message, providing an opportunity to suppress the fire sooner.

Disabled alarms are a frequent factor leading to large fire losses. The classic "low-battery beep" often led to homeowner's disabling their systems. With the improved technology, smart-home alarm systems are less likely to be disarmed, again, improving the likelihood of early detection and response.

A new tool in claims handling

One of the most overlooked benefits of smart-home technology for insurers is how the data provided can also assist in the adjustment of claims. The data from a smart system can provide valuable evidence of the cause and origin of a loss. As noted above, technology now exists to put sensors and alarms on or near major appliances. The data from those sensors can eliminate or implicate an appliance as the cause of loss. This information can be instrumental for determining coverage and pursuing subrogation.

If a smart home is equipped with video cameras, the claims handler can quickly inventory the home's contents before and after a loss. This should lead to more accurate and timely claim settlements.

Finally, insureds can link their smart-home technology to their insurer so that a smart system automates the first notice of loss.[3] Insurers know that claims handled quickly and efficiently are likely to be less costly. The smart-home technology can give the claims handler a head start in resolving these losses.

Concerns over smart technology

As with any new technology, there are still questions and concerns to address. For example, if the smart system itself is damaged, the cost to replace it will likely raise the cost of repairing a home that suffers a loss. It's also true that hacking is a risk of smart technology, creating a new type of loss. A vandal could damage a smart home by hacking into the smart system and turning off the heat, causing pipes to freeze and burst. These concerns are real, but homeowners and the carriers must weigh the relative risks and benefits.

Is it possible to quantify the benefits of smart-home technology and offer discounts to these homeowners? There's still much variability and lack of standardization in what constitutes a smart home. Claims managers and staff should talk to underwriters about instances when they see that a smart system mitigated or prevented a loss, or when a smart system helped the claims handler resolve a claim.

The impact of smart homes

Smart homes aren't going to eliminate insurance claims, but they'll mitigate or eliminate some types of losses caused by specific perils. This technology can also provide valuable data that helps a claims handler adjust a loss. As this technology advances homeowners and insurers will need to continue to assess the risks and benefits which may alter traditional loss frequency and severity.

For more information on smart homes, please contact your Swiss Re representative.

[1] *Homeowners and Renters Insurance*, Insurance Information Institute, http://www.iii.org/fact-statistic/homeowners-and-renters-insurance
[2] Ibid
[3] *Next Generation Insurance: Tapping Into the Intelligence of Smart Homes*, Cognizant, https://www.cognizant.com/InsightsWhitepapers/next-generation-insurance-tapping-into-the-intelligence-of-smart-homes-codex1411.pdf

© 2016 Swiss Re

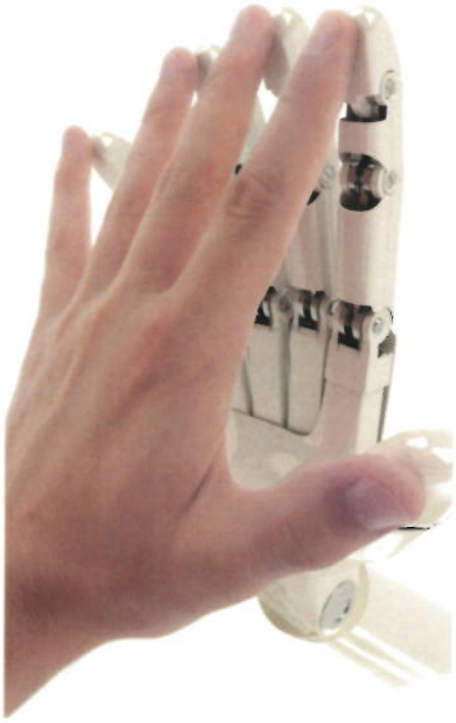
Swiss Re

Trend Spotlight

The robots are here: what that means for insurers

Have you read the news about robots lately?

It's hard to ignore the avalanche of headlines about the impact of transformative technology and robotics on business, industry, insurance, society and our personal lives. The onset of robotic capabilities and artificial intelligence (AI) is not a future issue, it is one to address now. In this paper, we will take a brief tour of the impact of these changes from the perspective of the insurance world.



The big picture

Collectively, we are facing a myriad of technological transformations, including the Internet of Things, smart homes, autonomous cars and, of course, robots. It has been estimated that "advanced robotics is going to thrust upon insurers a world that is extremely different from the one they sought to indemnify in the 20th century."[1] Other commentators have stated that new technology, including AI, is going to "unleash a new industrial revolution [that] is likely to leave no stratum of society untouched."[2] In response, roughly 30% of leading organizations will create a chief robotics officer role or a similar role for their business in the next two years.[3] Ready or not: the robots are here and more are coming.

What lines of business are affected?

Really, which line isn't affected? More and more robots introduce new coverage and/or liability issues for nearly every line of business in insurance. Key examples include: Commercial General Liability, Product Liability, Employment Practices Liability, Technology Errors and Omissions, Workers' Compensation, Cyber Coverage, Professional Liability, and Directors and Officers Liability, and, of course, stand-alone robotics policies. Bundled or hybrid policies that include many component coverages are attractive as one-stop offerings because insureds often prefer broad coverages (vs. numerous stand-alone policies). Bundled offerings can simplify purchasing and help reduce an insured's risk of insurance gaps.

What do we mean when we talk about robots?

Presently, there are two key categories of robots: machine-based, non-collaborative robots, which often work in traditional industrial or retail settings (think of a modern-day car factory or an Amazon warehouse), and collaborative open robots (also called 'cobots'), which use AI and can learn and interact with humans. While most insurers are familiar with traditional industrial robots in the workplace, robots are advancing to work alongside humans — or on their own. Robots are being used to make deliveries and investment decisions, interview job candidates, administer medical care, and even run hotels.[4] A hotel in Tokyo now uses life-like robots to check in guests and deliver room service. Robots are being programmed to detect cyber breaches (or cause cyber breaches). The wide scope of robots requires insurers to reconsider policy language that has not yet contemplated robotic exposures.

Definitions are critical

How do you define robot in an insurance policy? It's impossible to use a single definition — and definitions will vary widely depending on the type of robot, its function, the insurance product at issue, and the intended coverage. Examples from the marketplace demonstrate that definitions may include reference to what the robot can do (and by implication, what can go wrong). A real challenge will be deciding whether the introduction of complex automated functions may be considered robots for purposes of robotic coverage. For example, is an autonomous car, drone or other advanced device a robot? Is a complex industrial machine a robot – or, part of an automated process? The distinction between automation and robotics is murky, and will likely remain unclear. Policy language will be one of the first reference points for disputing parties to turn to for guidance about coverage. Moving forward, insurers do have an opportunity to shape the marketplace for robotic definition, intent and exposure.

Another concern is how multiple contributors to a robot (like manufacturers, software designers, operators, etc.) may be sued separately as liable entities. Contractual arrangements may clarify (or complicate) legal responsibilities.

© 2017 Swiss Re

Currently, the plaintiff's bar can be expected to file litigation in a wide swath in order to capture all potentially liable parties; this might include suing the manufacturer, the software developer, the robot owner or employer, the data-service provider, and technology and design professionals.[5] There will be increased coverage and liability litigation, and likely more defense costs.

Standards and regulation may help

The introduction of standards and regulations may provide manufacturers and employers with protection from liability that could help in the defense of a robotic accident. A number of organizations are actively working on standards and guidelines regarding the use of robots. There are proposals from the International Standards Organization (ISO), as well as the American National Standards for Industrial Robots (ANSI) and the Robotic Industries Association (RIA). It remains to be seen what legal requirements and regulations will be promoted by governments at all levels.

The current challenges

"Robots are the technology of the future, but the current legal system is incapable of handling them."[6] This emphatic statement highlights an active debate about how the law should treat robots. Should robots with AI be held responsible for their own actions? Experts, academics and legal theorists are weighing many liability concepts, including owner liability, agency theories, and corporate legal-entity theories.

A key concern for insurers is the lack of legal precedents with respect to how robotic liability will be handled by courts. This places even more pressure on insurers to identify what they intend to cover (or what they don't intend to cover) through policy language. Outside of the US, Europe has discussed whether robots should be considered 'electronic persons,' whether robots should be required to be insured, and whether they should even be possibly taxed.[7] These discussions recognize that unilateral robotic actions fall into uncharted legal territory.

What can we learn from existing robotics cases?

There are a handful of legal cases involving robotics. Many of these are in the industrial and medical arenas. In one case, a worker died in an Alabama auto parts manufacturing plant, where "[t]he robot restarted abruptly, crushing the young woman inside the machine," according to the Occupational Safety and Health Administration.[8] The worker had entered the robotic station to clear a sensor fault that had stopped an assembly line; the robot should have been programmed not to start if a person was inside the station, according to the case's argument. The manufacturing plant, as well as the designer, manufacturer, marketer and seller of the robot, have been named as defendants.

A common liability inquiry is whether an employee put himself or herself in the way of harm — creating a fault argument against the employee. Another liability question is whether the employer correctly followed instructions for the installation and operation of a robot. These are areas where workers' compensation policies have traditionally been available to address workplace injuries. But products liability claims may be filed in instances where there are allegations that a robot was defective in terms of design or operation. Consistent with traditional workplace exposures, Employer's Liability claims might also be filed where there is a failure to address workplace safety.

Are we paying enough attention to the impact of disruptive technology?

One concern about the onset of advanced robotics may be the lack of attention to the technology risk. 55% of organizations have not conducted risk assessments to understand the impact of disruptive technologies, according to a Marsh/RIMS 2017 study.[9] This is unsettling because it shows many companies haven't thought about disruptive technology, much less begun to deal with it. For these disruptive technologies, there is often little, if any, experience or loss information to provide guidance about traditional underwriting, pricing and claims-handling models. It will be imperative for insurers to devote time and resources to the assessment of risk issues presented by new technology. Insurers also need to consider the possible lack of risk assessment within their insureds' operations. Existing insurance policy terms and conditions may be outdated and inadequate because they don't contemplate robotic risks and exposures. As robotics and AI become pervasive, insurers have the opportunity to take a lead role in steering coverage through definitions.

Conclusion

Whether enough consideration is given to this topic can be debated. But insurers do recognize the gravity of the expected impact of AI and robotics: "75% of insurance executives believe that AI will either significantly alter or completely transform the overall insurance industry within the next three years."[10] Insurers must ask themselves if they want to be innovators or followers with respect to robotic coverages.

Assessments of robotic risk should include understanding insureds' current and future use of robots, and engaging in dialogue with insureds regarding safety, responsibility, supervision protocols and loss. Insurers need to pay attention to the current state of technology, and emerging case law and regulations.

A dedicated and iterative commitment will lead interested insurers to more successful underwriting and claims management. Insurers will need to revise policy language to keep up with evolving exposure and coverage issues. The rapid expansion of robots will force insurers to be agile in their recognition of the impact of new technology — and to thoughtfully assess and control risk on a line-by-line basis.

[1] http://insurancethoughtleadership.com/what-liabilities-do-robots-create/
[2] http://www.bbc.com/news/technology-38583360
[3] http://www.zdnet.com/article/the-future-of-robotics/
[4] www.asahi.com/ajw/articles/AJ201608050036.html
[5] https://blog.svlg.com/2017/01/06/stephen-wu-speak-global-artificial-intelligence conference/
[6] http://robohub.org/the-legal-issues-of-robotics/
[7] http://money.cnn.com/2016/06/22/technology/europe-robots-taxes-jobs/index.html
[8] http://nationalpost.com/news/world/alabama-factory-worker-dies-two-weeks-before her-wedding-after-being-crushed-to-death-by-robot
[9] https://www.marsh.com/us/insights/research/excellence-in-risk-management-xiv.html
[10] https://www.accenture.com/us-en/insight-insurance-technology-vision-2017; https:/ www.marsh.com/content/dam/marsh/Documents/PDF/US-en/Excellence%20in%20 Risk%20Management%20XIV-04-2017.pdf

Swiss Re

Trend Spotlight

The Internet of Things: a new landscape of hyperconnectivity and vulnerability

Technology is moving at an incredibly fast pace and it's difficult, but critical, to stay current on how these developments will affect the insurance industry. The Internet of Things (IoT) will be a key driver for exposure changes, emerging risk issues and new coverage questions. How do we begin to understand the implications? A starting point is to review the core concepts and capabilities of the IoT and then begin to assess the impact on insurance, including anticipating new claims and losses.

What is the IoT?

The IoT is the entire world of digital connectivity of objects as well as data flowing from those objects – it's the world of connected things. There are two categories of connected objects, "digital first" and "physical first". Digital first objects are built with digital sensors included, such as your smartphone. Physical first objects are built with sensors added later, such as a home alarm.

"Hyperconnectivity" is another word for the IoT, and it's probably a more descriptive word and one that helps us better understand the IoT. Essentially, while people have become connected through social media with vast quantities of social information, things themselves are increasingly connected and the data that they produce can be shared and analyzed in new ways. Insurers must be informed about what things are being connected and what data can be produced.

References to the IoT are inescapable in insurance industry journals, blogs and commentary. The IoT is so pervasive that it's recently been stated that the IoT is eating the World.[1] The IoT is fundamentally driven by connected devices, and it's estimated that by 2020 there will be 50 billion connected devices, seven times more networked devices than people.[2] How and why do all of these connected objects matter? Massive connections and data will change losses, risks, products and pricing.

Millennials may drive hyperconnectivity because connectivity is an expectation for all interactions. Future success for insurers

may depend upon their ability to differentiate themselves by embracing new data via IoT connectivity. Data collection, analysis and exposure assessment may also be critical pricing motivators that allow insurers to develop tailored products for a new generation of insurance buyers.

What's triggered IoT discussions now?

Connected objects have sensors embedded or attached to them. Sensors have become smaller and cheaper over time. Not all sensors are inexpensive enough to install across homes, bridges, industries and cities, but certainly they're routinely built in newer objects and increasingly attached to existing physical objects. Another important change is the continued advancement of the size and speed of communication networks and the ability to connect data through huge networks. The reduced size of sensors, economics of installation and network speeds will continue to accelerate the use of sensors across countless businesses, enterprises and systems.

Predictions for IoT impacts

With any new technology, there will be those claiming that the concept will revolutionize and reduce losses, as well as improve risk assessment. Yet, with any new technology, we'll trade some benefits for some new risks. A few key predictions are that digital risks will increase and product liability exposures will present some novel expansions. We expect standards to be proposed that will establish new manufacturing protocols which may help define security liabilities. Also cyber and hacking risks could increase the demand for cyber types of coverage. The inherent vulnerabilities associated with hyperconnectedness will magnify this demand. In addition, more

[1] "The IoT is eating the world, with some legal risks," *Solair*, Giulio Coraggio, April, 6, 2016. https://www.solaircorporate.com/en/iot-data-protection/

[2] *Living in a Hyperconnected World-Implications for the Casualty Re/Insurance Industry*, Swiss Re, 2014. http://media.swissre.com/documents/Living_in_a_Hyperconnected_World_Web.pdf

© 2016 Swiss Re

interconnectedness brings with it the threat of larger matrix types of losses, such as the disruption of a connected city system. Issues such as supply chain preparedness and accumulation control will be scenarios to anticipate and map in order to understand how losses may fan out as exposures and claims.

5 IoT areas and issues

Cars

Almost everyone is familiar with today's connected car capabilities such as collision avoidance, traffic efficiencies and the possibility of sensors to detect maintenance or repair issues. In addition, with increasing concerns about commercial motor and trucking losses, a sensor may be developed to detect driving problems, for instance to alert a sleepy driver to avoid an accident. However, the potential benefits of sensors tend to raise new issues about risks. A few of the risks associated with connected cars have also been widely discussed including the possibility of remote control by hijackers or whether sensors can make smart decisions when faced with multiple risk options.

Some commentators have suggested that the introduction of sensors actually increases liability risks for manufacturers vs drivers. The bigger question now becomes whether the mere occurrence of an accident will raise the presumption of a product defect. Sensor data might change presumptive fault concepts.

Deliberate exploitation is another new concern. There have been numerous hacking events against autonomous and manned vehicles, thereby raising questions about the level of security that manufacturers, software providers and tech companies should address. The plaintiff's bar will pursue liability arguments, particularly for breaches of electronic security. The issue of the acceptable standard of care for electronic security is quite new and raises a number of legal issues that are likely to play out in the courts, with insurance policies in the balance.

Homes

For connected homes there are three main areas of interest: appliances, security and infrastructure. Insurers may find new opportunities for risk selection and possibly greater opportunities to mitigate losses through early detection of common risks, such as water, fire or theft. As smart sensors are more commonly used for homes, data and usage will inevitably result in new pricing or discount structures. Additionally, some experts have suggested that insurers consider entering the market of smart home product offerings, or risk competitive disadvantages. Some insurers are already partnering with businesses that offer such products.

Cities

Sensors that collect information or provide energy savings are key features being installed in modern cities. Sensor installations that include cameras will raise privacy issues. There are other unique questions arising out of city installations, especially where these projects are undertaken in joint collaborations with other public or private entities and therefore raise questions about shared investments, ownership and data. The "hackability" of city sensor systems is a key concern and one which was investigated in a report by Lloyd's of London called "Business Blackout"[3] which predicted massive economic disruption and discussed policy provisions and coverage issues that might arise.

Wearables and medical technology

There are a number of theoretical applications that could potentially mitigate damages in the worker's compensation arena. However, there are also novel privacy-related issues that have already resulted in litigation. One matter involves an employee who sued her employer based on allegations that off-hours tracking intruded on her privacy rights. There are numerous reports of medical technologies, including insulin pumps and medical robots, that have been experimentally hacked. However, real hacks could implicate medical device makers, hospitals, design professionals and their insurers. Critical questions for employers including how will they use wearables or data, and what happens if the data is hacked?

Industrial Internet

The Industrial Internet, sometimes called M2M or Machine to Machine connectivity, may be one of the fastest advancing IoT areas and one where IoT concepts seem to offer a more immediate and tangible opportunity for savings, risk prevention and efficiencies. Unfortunately, the contrary is also true which is that where connected devices have failures or defects, this will result in losses and insurance claims. Huge scales of damage or disruption could occur because of hacking, sabotage or digital failures. Industrial IoT sabotage raises questions about terrorism exclusions, cyber coverage and determinations regarding the number of events or occurrences. Incidents of industrial sabotage have already been well documented[4,5] and should motivate carriers and their underwriters to evaluate the extent of intended coverage under existing policy language.

Anticipating the future and remaining competitive

Beyond line of business considerations, insurers need to stay alert to remaining competitive as data-rich entities consider offering traditional insurance. The IoT will cause new causes of action to emerge, create new liabilities and result in unconsidered and unanticipated insurance claims. There are a number of entities developing regulations, but this landscape is also fragmented and inconsistent. For product liability issues, there's much uncharted territory for what's "reasonable" or even "defective" when it comes to connected products. Will "hackability" itself be recognized as a viable cause of action?

Conclusion

Lloyd's of London estimated a value of $5.5 billion in coverage disputes for a large hypothetical East Coast blackout.[6] Insurers must review existing policy language to consider IoT scenarios to determine what they intend to cover or exclude. The ambiguity of coverage issues will make claims potentially longer in duration and more expensive to defend. The IoT presents vast new liability issues ranging across key product lines: product liability, cyber, terrorism and technology. The sheer number of connected things raises the specter of MDL and class-action litigation. Supply chain disruptions and connected city scenarios could trigger accumulation risks. Successful insurers will invest time understanding how uncontemplated IoT scenarios may increase exposure. In addition, in order to remain competitive, insurers will have to employ connected data to improve risk selection, pricing and loss mitigation.

[3] "Business Blackout: The insurance implications of a cyber attack on the US power grid," *Emerging Risk Report – 2015*, Lloyd's and the University of Cambridge. http://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf

[4] "Shades of Stuxnet: Newly found malware can sabotage industrial controls, but only in simulated environments," *SC Magazine*, June 6, 2016. http://www.scmagazine.com/shades-of-stuxnet-newly-found-malware-can-sabotage-industrial-controls-but-only-in-simulated-environments/article/500887/

[5] "A cyberattack has caused confirmed physical damage for the second time ever," *WIRED*, Kim Zetter, January 8, 2015. https://www.wired.com/2015/01/german-steel-mill-hack-destruction/

[6] "Business Blackout: The insurance implications of a cyber attack on the US power grid," *Emerging Risk Report – 2015*, Lloyd's and the University of Cambridge. http://www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf

Swiss Re

Trend Spotlight
Drones

The commercialization of drone technology has virtually exploded over the past few years, and the global use of drones is expected to have enormous future implications. Insurance coverage for drone operation is an essential aspect of this technological evolution.

What is a drone?

Drones come in a variety of sizes and types, from model aircraft for personal use to large, fixed winged aircraft used by the military. The International Civil Aviation Organization (ICAO) has set a new definition referring to drones as RPAs (remote piloted aircraft systems). Model aircraft are distinctly different from RPAs as they're used purely for recreational purposes.

First arising as a result of military conflicts, RPAs became much more sophisticated after 9/11. At least 50 other countries use RPAs, and there's also evidence that some terrorist organizations may operate RPAs.

Amazon made headlines when it petitioned the Federal Aviation Administration (FAA) to use RPAs to deliver packages, but Amazon is not alone. Annual spending on aerial RPAs, including civilian and military applications, is projected to reach $11.6 billion in 2023 (up from $5 billion in annual spending now). Over the next ten years, the Teal Group forecasts nearly $89 billion will be spent on RPAs globally.

Advantages for the insurance industry

Insurance is just one industry that could benefit from the use of RPAs. For example, after a natural catastrophe, an RPA could reach a remote scene much faster than a claims adjuster. Details of a risk could be validated without travel costs or in-person inspections. Instead of climbing a ladder, a claims adjuster could dispatch an RPA to investigate an icy patch of a damaged roof – drastically saving costs associated with claims adjusters' workers' compensation claims.

Special exceptions

Since 2005, Predator RPAs have provided border surveillance in the US. RPAs have been used for aerial reconnaissance, aerial policing and crowd monitoring. In 2014, the FAA approved the first large-scale commercial RPA operation in the US, along Alaska's northern shore. The RPAs collaborate with researchers in gathering real-time data from one of North America's largest oil fields. These same RPAs could be used to map the path of future oil spills. In Australia and Japan, RPAs are used in agriculture to study crop yields, survey property, tailor the use of herbicides, pesticides and fertilizers. In Canada, RPAs are flown over potato fields to collect information that may help farmers reduce spraying and increase yields. The use of RPAs for science and research is virtually limitless.

Real-estate photographers use RPAs to shoot aerial shots of residential properties (despite the federal ban in the US on such use). These lightweight radio-controlled helicopters shoot photos and videos that show homes in context to neighbors, golf courses and other landmarks. In Canada, realtors have used RPAs dramatically; after flying around a large exterior space, the RPA flies through the front door into the home for sale.

RPAs have been hailed as the future of journalism – safely reporting on riots or fires. In 2014, the FAA approved exemptions for the use of RPAs in the film and television industry. Disaster management, search and rescue missions and humanitarian efforts are additional uses for RPAs.

With a cost as low as $20, hobbyists have bought RPAs in record numbers. In fact, in December 2014, the FAA published a video – highlighting regulations for recreational use – just in time for those who received RPAs as holiday gifts.

Potential legal issues

The Federal Aviation Administration has been working for several months to implement "Special Rules for Certain Unmanned Aircraft Systems," intended to regulate commercial operations in low-risk, controlled environments. While making progress, the FAA may not meet the September 2015 deadline due to significant technological, regulatory and management barriers. Until the FAA issues its "Special Rules," commercial RPA operators must apply for and receive permission to operate RPAs in national airspace. The operator must obtain a Certificate of Waiver or Authorization from the FAA as well as a "Special Airworthiness Certificate" (just like any other aircraft).

In one case, the FAA issued a cease and desist order and a civil penalty on a commercial operator. This case arose after the University of Virginia paid an advertising firm that hired Raphael Pirker to fly a model airplane equipped with a camera to take video and photos of its campus. The FAA levied a $10,000 fine against Mr. Pirker for flying his "aircraft" too close to people and buildings, asserting that Mr. Pirker violated an FAA regulation which prohibits the careless or reckless operation of an aircraft. Mr. Pirker appealed the order to an administrative judge who ruled against the FAA.

© 2015 Swiss Re

The FAA appealed the *Pirker* decision to the National Transportation Safety Board which issued its ruling in November 2014. The NTSB ruled that the regulations giving the FAA authority over aircraft didn't expressly exclude model aircraft. Therefore, the FAA can enforce the prohibition on careless and reckless operation of an aircraft as outlined in its regulations. The NTSB didn't rule whether the FAA has issued valid regulations regarding commercial use of model aircraft. Until a court of law rules otherwise, the FAA will likely assert that it does have authority to ground commercial use of model aircraft.

The FAA generally limits operations for hobby and recreation to below 400 feet, away from airports and air traffic, and within the sight of the operator.

Privacy concerns

One of the principal concerns with RPA use is citizens' privacy. In the US, states have taken the lead to regulate this issue, resulting in a patchwork of legislation varying from state to state. According to the ACLU, as of June 2014, 13 states have enacted some form of legislation prohibiting RPA use over private property without the consent of the owner. Similar legislation has been introduced in 36 other states.

Meanwhile, Canada has quietly allowed use of commercial RPAs since 2007. Transport Canada, the federal government entity that oversees the operation of RPAs for commercial purposes, requires RPA operators to obtain a Special Flight Operation Certificate before flying an RPA. Furthermore, RPAs are subject to Canada's Personal Information Protection Electronic Documents Act which requires permission of a person to take his or her photograph or video.

Other potential legal issues raised by RPA use include physical damage and bodily injury, trespass, nuisance, stalking, harassment, wiretap laws and abuse by law enforcement.

Underwriting challenges

Present policy wordings may not address the issues arising from commercial use of RPAs. Carriers may wish to limit their existing policies or draft new policies tailored to a particular insured's needs. Some of the general types of coverage that may be needed for the commercial use of RPAs include:

- Property insurance including machinery breakdown and business interruption
- Commercial general liability for non-airborne liability exposures
- Personal injury (including invasion of privacy coverage or not)
- Aviation liability
- Non-owned aviation liability
- Professional liability
- Workers' compensation (in the US)
- D&O liability
- Umbrella liability

The ISO responds

The ISO's Commercial general liability policy includes several provisions that expressly address coverage of aircraft. For example, the aircraft exclusion in Coverage A excludes bodily injury or property damage arising out of the ownership, maintenance use or entrustment to others of an insured's aircraft.

Coverage B, however, doesn't contain an exclusion explicitly addressing aircraft. Thus, as currently written, the CGL policy may provide coverage under Coverage B for a claim alleging violation of privacy arising from the use of an RPA.

In response, the ISO has developed several optional endorsements addressing liability exposure of RPAs for commercial purposes. These endorsements will become effective in June 2015 and will modify coverage under the ISO's commercial general liability and umbrella and excess policies.

Intended to provide underwriters with flexibility to tailor coverage as needed, the endorsements range from excluding all unmanned aircraft to excluding coverage under either Coverage A only or Coverage B only of the CGL policy. Additional endorsements specifically limit coverage for designated unmanned aircraft as listed in a scheduled endorsement.

Although technology is advancing at break-neck speed – RPAs as small as mosquitoes have now been developed – wide commercial use of RPAs hasn't kept pace. The commercial RPA industry in the US is in a holding pattern awaiting the FAA's much-anticipated regulations.

For more information, contact your Swiss Re Claims Representative.

References:

FAA Advisory Circular 91-57, Model Aircraft Operating Standards, http://www.faa.gov/documentLiabrary/media/Adivosry_Circular/91-57.pdf

Insurance and the rise of the drones, Swiss Re, http://media.swissre.com/documents/2014_12_rise-of-drones.pdf

NTSB Order No. EA-5730, http://www.ntsb.gov/legal/pirker/5730.pdf

© 2015 Swiss Re