Chapter 16
The Insurance Industry—Cyber Security in the Hyper-Connected Age

Apoorvaa Singh and K. B. Akhilesh

Abstract The insurance sector forms the backbone of the global economy, because it enables both individuals and firms to undertake risky endeavors, which they would otherwise have avoided. As former Cisco CEO John Chambers put it, “the Internet of Things will be bigger than the Internet.” This truth has not been lost on the insurance industry players. In anticipation of the efficiency in operations and reduction in costs that technologies like artificial intelligence, cyber-physical systems, etc., promise to bring, insurers are already beginning to change their endgame by incorporating these technologies in day-to-day operations, building new insurance products, services and business models. But with each new technological breakthrough, the risks also change form. Currently, the risks are manifested in the form of the threat of cybercrime. To effectively tackle this threat, insurers will need to take a deep look at their underlying systems and process, and at the unnamed enemy’s modus operandi as well. We first take a look at the soft spots and threats faced by the insurance companies, and the impacts of these threats. We find that both management and technology measures are necessary to tackle the threat. We then come up with a five-pronged recommendation framework on how insurance companies can strengthen their security infrastructure.

16.1 Introduction

Insurance, as a function of trade and society, traces its origins back to as far back as the second and third centuries BC. It is meant to provide protection from risk of loss, usually in the form of financial aid enabled by premiums paid by the insured person in the past. It can be seen as a form of hedging against the risk of some uncertain, contingent loss.

A. Singh (✉)
Financial Consulting, Mumbai, India
e-mail: apoorvaa.singh30@gmail.com

K. B. Akhilesh
Department of Management Studies, Indian Institute of Science, Bengaluru, India
e-mail: kba@iisc.ac.in

K. B. Akhilesh and D. P. F. Möller (eds.), *Smart Technologies*,
https://doi.org/10.1007/978-981-13-7139-4_16

Today, this industry forms the backbone of every action that involves risk—from major business transactions to actions as simple as the buying of a car, or travelling to a city located mere miles away.

In 2016, the global insurance industry was worth 4 trillion US dollars, in terms of gross insurance premiums. With the improved economic growth and bull markets in Asia, Australia, Americas and Europe, all major audit corporations like KPMG, Deloitte, PwC, Accenture, EY, etc., say that the valuation of this industry will grow further in 2018.

Traditionally, the insurance sector has been slow on the uptake of technology, compared to its faster-moving financial services industry counterparts like banking. This trend is slowly but steadily changing—insurance, too, is finding the potential benefits of IoT and AI difficult to resist. More than just improvement in efficiency, these technologies are opening up new avenues and business models for the industry. And as with any new breakthrough in the curve of technology evolution, the threats too are evolving. Cyber security is a looming issue like never before—the World Economic Forum listed data fraud, technological infrastructure breakdowns and cyber security incidents among the top ten risks faced by the global economy. Even the insurance industry CEOs are sitting up and taking notice—according to a KPMG survey, insurance CEOs admitted that they thought cyber security risk outweighs any kind of regulatory risk (KPMG 2017).

Before launching into a detailed discussion regarding the cyber security risks facing the insurance sector, how and why these risks arise, and recommendations to overcome them, we first discuss the workings of this sector in brief.

16.1.1 How Insurance Works

The organization or entity which gives insurance as a service is called insurer, insurance carrier or insurance company. The individual or setup to which the insurance is sold is called the policyholder, or alternatively, the insured. The insured pays a fee in the form of premium to the insurer, while the insurer gives a verifiable promise to compensate the insured for a covered loss if it arises, in lieu of the regularly paid, agreed upon premium. All terms and conditions are established in a contract known as the insurance policy. The covered loss must always be explainable in financial terms and should be such that the insured can establish a direct link between the loss and themselves. Before the insured can get the assistance set forth in the insurance policy in case the covered event does happen to occur, they must submit a claim to the insurer, which is then processed by a claims adjuster.

The way the insurers run their business is to pay out less in loss coverage, compared to what is collected by them through premiums and income earned by investing the premiums collected. They also offer competitive premium prices such that these will be accepted by the consumers. Profit for the insurers is, thus, through earned premium and investment income, less the incurred loss and underwriting expenses.

The marketing is usually done by insurance agents who leverage their network of contacts to solicit new clients. Broking firms, banks and other organizations like NGOs, etc., may also tie up with insurance companies to promote their schemes to their client base.

Broadly speaking, the insurance market can be divided into 12 types: vehicle, gap, health, disability, worker's compensation, political risk, crime, life, burial, property, liability and credit. There are other types of specialized insurances as well, like loan, education, travel, expatriate, pet, pollution, interest rate, etc.

16.1.2 Modern Insurance Process

The modern insurance process broadly consists of the following stages: product design, pricing and underwriting of the said product, its distribution, administrative tasks and claims management. Each of these steps involves a number of stakeholders other than the insurance company and the end client. Figure 16.1 illustrates the process steps and the external stakeholders involved at each step.

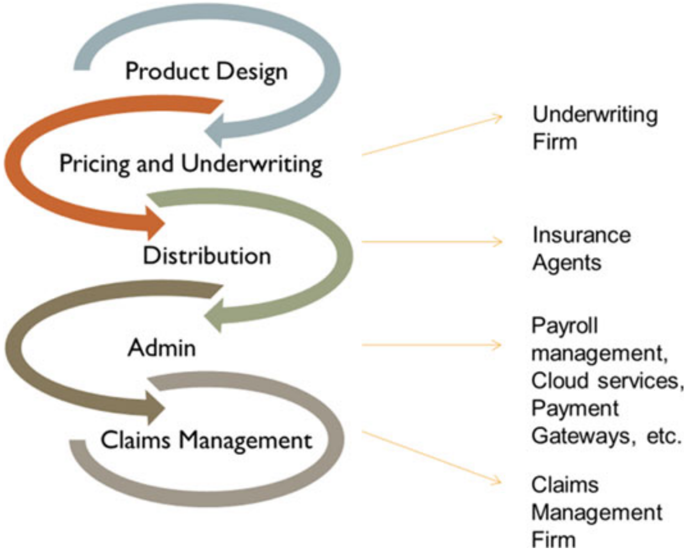


Fig. 16.1 Modern insurance process and external stakeholders involved

16.1.3 The Indian Insurance Market

The formal Indian insurance sector came into being with the setup of the Oriental Life Insurance Company in Kolkata in 1818. It comes under the Union List of the Constitution of India, implying that only the Central Government can make policy decisions regarding this sector. Since Independence, it has undergone a full cycle of governing policy changes, from being an unregulated sector to fully regulated, and now, partly deregulated.

By the year 2012, the Indian insurance industry was worth US$72 billion. But overall, only around 0.2% of the population has any kind of health or life insurance. The scope for further growth is therefore huge for the traditional insurance products. The growth potential is also aided by the fact that more and more private players with specialized services are starting to carve their own niche in this sector. Due to Internet penetration, products like micro-insurance and online policy purchase have become popular (EY 2010; IBEF 2018).

16.1.4 The Economic Impact of Insurance

The insurance sector helps any society in the way that it enables rapid recovery from losses and facilitates risk-taking ability. In India, the insurance sector has had another major role to play—in the country's economic development. Since majority of the players in the insurance market in India have historically been either wholly or partly owned by the government, their financial corpus has been used to provide long-term funds to the government for infrastructure development and welfare schemes.

16.1.5 Peculiarities of the Insurance Sector, in Comparison with Other Financial Services Sectors

Traditionally, insurance companies have been established with huge pockets. Mergers, acquisitions and consolidations have ensured only a few big players remain on the scene always. But in the last decade, startups using technology to drive down costs and improve efficiency gaining ground in terms of acceptance by end consumers and market share.

The other peculiarity of this sector is that insurers never work in isolation. Each insurance company is surrounded and supported by a nexus of external agents in its operations. The major stakeholders include policyholders, shareholders and investors, regulators, tax authority, credit rating agencies, brokers and tied agents, claims management firms, underwriters, reinsurers and other third-party services.

16.2 The Present Tense: Insurance, Technology and Such

Traditionally, the insurance sector has not been as quick on the uptake of new technologies as the other financial services sectors like banks and trading. Client engagement has been low historically, with end customers solicited through phone calls and third-party agents. Paperwork is still prevalent. But the times are a changing.

In the last decade, Internet-based communication and solicitation, big data, digital data storage, data analytics, cloud computing, etc., have become the norm. An offshoot of these technologies has been the creation of new insurance products (like cyber insurance, hyper-micro-insurance, etc.), and new business models, channels and services (like InsurTech, Peer-to-Peer insurance, etc.). The most prevalent technologies in the industry today are discussed below in brief.

16.2.1 Data

Data, especially, is driving immense changes in the insurance industry. Insurers are increasingly leveraging data and advanced analytics to help increase the transparency in the conduct of day-to-day transactions, make risk models more robust by fine-tuning the occurrence probabilities of known and unknown risks. Data science is also being heavily utilized by underwriting agencies to detect patterns of fraud and gaming of the system by long- and short-term contractors—Toyota is in fact utilizing analytics for identifying fraudulent and unethical behavior of its associate suppliers for a very long time. Using analytics can also lend greater insight into the needs and wants of the end consumer—this will help in coming up with new products and services. The technology curve has only grown steeper with time—so companies will need to keep pace with their end consumers' propensity for technology if they wish to stay relevant. In recent years, a prime example of this has been the creation of cyber insurance policies.

With the help of data, insurers are gradually moving from the phase of risk management to risk prevention. It is anticipated that Internet of Things will enable insurers to help their consumers monitor their surroundings and therefore to be pre-warned about any risky events that may occur. Insurers can warn consumers about old pipes that have reached the end of their lifetime, cyclones, safe shelters around their location in the event of facing a storm while out on travel, etc. Another impact of the use of technology and data will be greater personalization of services with respect to each individual consumer.

16.2.2 New Insurance Products, Especially Cyber Insurance

The highly connected digital world has presented as many opportunities for cybercriminals as they have for businesses the world over. Larger corporations usually have robust infrastructure and policies in place to deal with cyber incidents. This may not be the case for small and mid-sized businesses. They often use third-party systems for services like payment gateways, data storage, etc., thereby increasing the number of potential backdoors. Also, the increasing use of IoT devices and artificial intelligence in day-to-day operations by businesses is expected to give rise to new liability clauses.

With laws and policies to deal with data protection and ownership, IP rights, cyber incidents and associated liability still in their infancy in many countries, including India, a new product niche has been created—cyber insurance to hedge the risks due to unforeseen cyber incidents (Moynihan 2018; Singh 2014). According to a report by Allied Market Research, this market will reach US$14 billion by 2022. But to build and maintain credibility in this rapidly growing market, the insurers will have to first get their own house in order, with respect to their internal cyber risk management activities and policies.

16.2.3 Digital Platforms

In the age of Internet, it is no wonder that insurance too has moved onto the digital marketplace model. The outcomes of this in terms of innovation in the business model can roughly be classified into three types. First, insurance aggregation and management platforms like PolicyBazaar have become extremely popular. These allow consumers to compare aggregated policies from different insurers, apply online, keep track of documentation and apply for claims on the Web site itself. Second, peer-to-peer insurance platforms allow a group of strangers to pool together resources to buy policies at comparatively lower rates than they would have if they bought the policies individually. This can be achieved either through brokers acting on a specific group's behalf, or individually through direct carriers offering such schemes which then group the individual policyholders internally. Policyholders pay a part of the premium into a common pool that covers minor losses, and the rest of the premium to a standard policy. If any amount remains in the pool after claims adjustment for the year, it is paid back to the policyholders the next year. Third, insurers allow consumers to purchase on-demand, usage-based micro-policies online—for example, an Airbnb homeowner may purchase policy for one night of rental of her property.

The above business models are collectively grouped under the umbrella term of InsurTech. The InsurTech space has seen many startups in the past few years which are heavily leveraging data, technology and machine learning to cover niches and gaps left un-touched by larger, more traditional insurance corporations. These startups are also leveraging technology for other areas of the insurance value chain—like finding the right mix of policies to complete an individual's requirements, pricing policies, uncover patterns of misuse and fraud, automated claims processing and adjustment, etc., (EY 2010). They have lower legacy costs and greater agility as well as flexibility in terms of business models, compared to the bigger firms—this has actually proved to be a great competitive advantage for them in an industry that has historically favoured players with deep pockets. One proof of their rising dominance is the level of global investment in InsurTech startups—it rose from $740 million in 2014 to more than $2.6 billion in 2015.

16.2.4 RegTech

RegTech is another area in which insurance industry startups are creating waves. By definition, these startups are leveraging technology to make the increasingly stricter compliance and regulatory requirements since the 2008 financial crisis, much more easy and intuitive to follow for the insurers. They are working toward data aggregation from multiple sources including social media and smart appliances used by the consumers for the purpose of building robust risk profiles and consumer profiles, modeling of risk for the purpose of stress-testing, asset management, detection and prevention of money laundering and fraud, automatic updation of compliance manuals with each new legislation that is formulated and implemented, etc. For these purposes, they are using natural language processing, optical character recognition readers, machine learning, sentiment analysis, pattern recognition, biometrics, etc.

16.3 The Future Tense: Trends in Technology, Originating in Other Sectors, Which Are Set to Impact the Insurance Sector

Since the past few years, insurers are looking at more advanced technologies like the Internet of Things, artificial intelligence, telematics, global positioning system (GPS), blockchain, drones, smart contracts, etc. These are innovations taking place in sectors other than insurance.

Any insurance policy is aimed at hedging risk associated with a given task. As the face of the sectors which solicit insurance change, so will the kinds of risks they face and the associated insurance policies they need. Thus, these technological innovations in other sectors are beginning to impact, or will impact in the future, how insurers work and build relevant products and business models.

The interest in these technologies has also been driven by the promise of cost savings and operational efficiency that they seem to hold—both for the insurer and for the insured. These technologies are currently being prototyped to come up with new ways to control, measure and put an efficient price on risk, automate fraud detection and claim processing, interact with consumers, etc.

16.3.1 Smart Homes

With the advent of smart home monitoring systems utilizing IoT, insurers and end consumers have greater control over risks through access to real-time data and intelligent monitoring algorithms.

For example, Oaktor, an Indian startup based out of Noida, manufactures smart plugs, plugged-in sensors and a mobile app to monitor these. The combination provides the homeowner remote control over the settings of multiple devices like refrigerator, TV, water heater, lamps, etc. This helps mitigate the risk of property loss due to electric device misuse. Another Bengaluru-based startup, Silvan Innovation Labs, manufactures smart door monitoring devices—these can help mitigate the risks of break-ins (Sangwan 2016). Google's subsidiary Nest is also in the home automation space. Some insurance players have started incentivizing their clients for purchasing and installing such products—American Family Insurance, for example, offers its policyholders $30 discount on purchase of home monitoring devices from certain companies and a further possibility of 5% savings on policy. The rationale is that smarter homes will see a dip in the frequency and severity of risks and therefore claims (IIF 2016).

16.3.2 Cyber-Physical Systems

Cyber-physical systems like unmanned drones are increasingly being used by insurers for surveying isolated or dangerous territories which have recently experience natural or man-made disasters, for the purpose of assessing losses and further speeding up loss adjustment claims processing. For example, Allianz used drones to assess the damage in the flooded areas of southern Germany in 2017, for assessing the damage done.

16.3.3 Intelligent Health Care

Wearable biometric sensors and use of artificial intelligence are transforming health care by reducing risk to healthy living by leading a change from the practice of healing existing ailments to preventing ailments. Devices like Fitbit are making health care more "personalized, predictive and preventive," according to a report released by PwC. For example, doctors in the future will be able to mine and analyze real-time and historical patient data using artificial intelligence to predict the occurrence of an ailment much before it actually occurs. Such data will include the patient's entire medical history, medical images, genetic makeup, etc. According to IBM, by 2020, medical data will double every 73 days—meaning there will be no dearth of this valuable resource. A similar report by Frost and Sullivan says that AI healthcare applications have the potential to improve treatment outcomes by as much as 30–40%.

The promise of reduced health risk is definitely catching the interest of the insurance companies. They are already beginning to utilize wearables to encourage and reward their policyholders for adopting healthier lifestyles and reducing their risk of developing lifestyle disorders. An example is the South Africa-based company Vitality Group, which, according to their Web site, provides policyholders personalized health goals. The end consumers are provided with automated tools connected to the cloud, in which they can easily log their daily activities. These logs are connected to personal healthcare technology at the backend and are used to provide real-time insights to the consumers, their family members and physicians (IIF 2016).

This trend is only set to grow further as meticulous health care becomes prevalent. It is anticipated that as diagnosis, treatment and prevention of ailments improve, people will visit hospitals with less frequency, thereby reducing cost to insurers in the form of claim costs.

16.3.4 Autonomous and Connected Cars

Autonomous and connected cars are yet another technological revolution that is anticipated to impact car insurance products, coverage and policies. Fully driverless cars reaching the roads are a reality that will still take at least a decade to fulfill. But the rapid pace of research and development by companies like Google, Tesla and nuTonomy is making insurers look closely at the scenarios that autonomous and connected cars may create for which new products and policies may be needed.

Various studies have found that driver error is the topmost cause for car accidents—autonomous cars in their stable avatar will effectively remove humans from the navigation controls of a car, thereby reducing driver errors. Market observers anticipate that reduction in driver errors will also lead to a corresponding drop in insurance claims.

But the flipside to the above potential positive was witnessed in the death of Joshua Brown while driving his Tesla Model S in autopilot mode, in July 2016. His car mistook an oncoming white lorry as the bright sky. This raises questions over how and to whom responsibility will be assigned in such cases—will it be the software, the driver, the bystander who unintentionally befuddled the car's AI or the manufacturer? It is highly possible that the future car will be a combination of both human and software interactions—how, then, will the responsibility be split in the case of any untoward incident? (IAIS 2016).

But before the day of perfect autonomous cars dawns, technological enhancements to a car's systems are already leading to safer roads. Examples include automatic braking systems, staying alert, lane-keeping, safe distance systems, etc., by Volvo and Tesla.

Insurers like Octo, MyDrive Solutions and Metromile are already looking at ways in which technology used in today's cars can be utilized. They are using data collected through telematics, GPS, mobile phones, etc., to build and assess a potential customer's risk profile (IIF 2016). Examples of new assessment points on driving habits generated from telematics include real-time data on number of abrupt turns taken, speed at which person drives at what time of the day and how frequently, etc. A report by Markets and Markets says that automotive and insurance companies have been extremely quick in applying telematics-based solutions to insurance products and services. The direction of these solutions so far has largely been for modifying and monitoring the behavior of drivers on the road, to make assistance seeking while on the road simpler and easier, and to manage claims in a more efficient manner.

16.3.5 Blockchain

Blockchain is the technology underlying Bitcoins. It provides for a distributed consensus system among a given set of parties to enable the quick validation and secure execution of inter-party transactions. It does not require any trusted central authority because of the security nexus formed by cryptography algorithms, computational power and the network of users required. Since the transactions recorded on the blockchain are immutable and because virtually any kind of information can be stored in a digital format, blockchains are already changing the way in which transaction ledgers are maintained. This has implications cutting across various industries.

The insurance industry needs meticulous transaction storage and retrieval for tasks like client risk profile building, claims processing, etc. Ernst and Young, in its 2017 quarterly report on the insurance industry, states that blockchain technology has the potential to do away with mistakes due to human negligence and also helps detect instances of fraud. This will be possible because blockchain will create a digital data store that reflects a common, agreed upon truth at all times—this database can then be used to quickly and effectively verify any claims and policy contentions (EY 2017).

It will also cut down on many back-office tasks, thereby improving the efficiency of operations. Claims will be processed faster through the distributed blockchain of entities involved in an asset's lifecycle, banks, insurers, underwriters, government authorities, etc. An example is the London-based startup Everledger, which is building a digital ledger for tracking the transactions of more than 8 million precious gemstones worldwide—they anticipate that their database can be utilized by insurers and claimants to enable faster claim processing. Also, since the transactions on the blockchain are time-stamped, it will also enable faster verification of a common truth and cut down on fraudulent claims—frauds globally cost insurers $60 billion each year.

Apart from the improvement in cost and efficiency, it also has the potential to make automatic insurance a possibility—a car purchase by an individual will trigger an automatic insurance policy purchase according to her profile and preferences, through the blockchain-based smart contract nexus of the car and insurance industries. It will also enable the automatic triggering of claims processing should a covered risky event, like hailstorms affecting crop growth, come to pass—through the use of smart contracts. Another use case is being developed by the P2P insurance company Dynamis—it is utilizing smart contracts on Ethereum blockchain to allow policyholders to pool funds and support each other monetarily if any incident happens (IIF 2016).

Insurers are definitely looking at blockchain with much interest—with various international consortiums like R3 and blockchain market initiatives coming up in the past few years.

16.3.6 Artificial Intelligence

Artificial intelligence (AI) is about allowing software to emulate human-like cognitive power. The use of this technology basket is set to pervade every other industry, from health care to transportation, and therefore will have an impact on the future directions that the insurance industry takes. For the industry itself, AI in its infancy, in the form of data mining and machine learning, is providing operational and cost efficiency already. It will enable all and more of all the functions discussed so far under the other technologies.

16.4 Insurance Sector in the New Age, Technology Savvy India

FinTech is one of the fastest growing sectors of the Indian startup scene, both in the number of startups and in the share of investment money received. The InsurTech scene, a subset of the FinTech sector, had the second highest number of startups coming up in 2016, after the payments sub-sector. In India, the InsurTech space is focused more toward the business model of policy aggregation than towards other verticals like underwriting, fraud detection or regulation compliance technology.

One of the oldest and most well-established InsurTech startups in India is PolicyBazaar, founded by Alok Bansal and Yashish Dahiya in 2008, in Gurgaon. It was among the first online policy aggregator and comparison Web sites in India. It is presently the market leader with nearly 70% market share. It made a net profit of Rs. 50 crore in the financial year 2016–2017. It has also been the securer of the largest funding ever in the InsurTech segment in India (at $85.3 million) and is currently valued at $100 million (Gooptu 2017).

16.5 Cyber Threats: New Age and Some Old

The insurance sector has never before seen the urgency that other financial services sectors see with respect to the immediate impact of the effects of cyber-events on their bottom-line, property and customers. The levels of technology needed for execution of day-to-day tasks have also been lower for the insurance sector traditionally. An insurance policy claim can be investigated for days together by human experts pouring over its clauses and supporting documents, before it is granted, while a trader relies on quantitative algorithms to make a decision to buy or sell within a split second. Cyber-criminals too have traditionally chased financial institutions from which they could derive instant monetary gratification—like banks. With the resulting lack of urgency for the insurance sector, this sector has been relatively slow in embracing technology. Therefore, the advance in cyber-enabled capabilities and the corresponding development of resistance against cyberattacks were been lackluster for this industry.

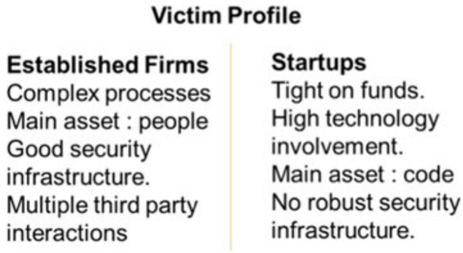
But data is the new gold, and the insurance companies are sitting on massive piles of pretty sensitive data—all insurers collect sensitive and confidential data related to health, finances, assets, transactions, etc., of their collect. They also share this data with third parties on a daily basis—these third parties being reinsurers, insurance intermediaries, etc. Also, the evolution of the market has been such that digitalized services and interactions are now a necessity, and not a luxury, to be provided by the insurance companies to their customers. As a result, insurers are now the new soft targets for cyber-criminals, as the other financial sectors have already built up strong cybercrime resistance focus and capabilities.

Before moving further, we first reiterate the definitions of the terms cyberattack and cyber incident. Cyberattack, as per the US Federal Financial Institutions Examination Council (FFIEC), is any attempt to access any electronic system or network, with the intention to disrupt or damage it. Such attacks harm data integrity for the organization targeted, steal information, control information flows and computing environments for adverse purposes, destroy and disable computing infrastructure through the cyberspace route.

Similarly, FFIEC defines “cyber incident” as any action or incident that has a negative effect on data, information and/or their storage systems, with that action having been undertaken by utilizing computer networks.

16.5.1 Recent Cyber Security Incidents

A group known as DD4BC has been active since around 2015, targeting financial corporations in USA, Canada, Australia and Europe. Their modus operandi is to extort ransom in the form of Bitcoins, with the threat of launching distributed denial of service attacks once a specified date passes.



Victim Profile

Established Firms
Complex processes
Main asset : people
Good security infrastructure.
Multiple third party interactions

Startups
Tight on funds.
High technology involvement.
Main asset : code
No robust security infrastructure.

Fig. 16.2 Cybercrime victim profile

The Axa Insurance Web site was hacked in September 2017, with nearly 5400 customers affected. Leaked information included the customer's e-mail address, date of birth and the mobile number which was used to transmit one-time passwords (OTPs).

The largest ever security breach, till date, surrounding an insurance company took place on February 4, 2015. Anthem Inc. lost over 78.8 million personally identifiable consumer health data, when its servers were broken into by hackers. The company lost a record amount of $115 million in payouts for the ensuing lawsuits.

Another incident was the hacking of the servers of the UK-based travel insurance company Staysure in January 2014. The three-digit Card Verification Value (CVV) numbers of over 93,000 people, who bought policies prior to May 2012, were stolen (BT Online 2017; IAIS 2016).

16.5.2 Victim Profile

The incidents listed above highlight that no one is safe—neither the technology savvy, new-age startups, nor the insurance industry behemoths with years of experience and standardized processes on their side. Figure 16.2 lists the characteristics of both the established firms and startups that may make them prone to cyberattacks.

16.5.3 Attacker Profile

The attackers can be classified into hackers operating for financial gain and hacktivists operating for sociopolitical purpose, based on their purpose. Knowing the purpose gives cyber resilience teams leverage on how to handle the criminals if the incident is already underway.

Based on attack range, KPMG calls for a 3-factor classification into commoditized attacks, targeted attacks and high-end attacks (KPMG 2017).

16.5.4 Soft Spots

In general, the insurance sector faces cyber risk from both internal and external sources, because they interact with multiple third parties and external agents on a daily basis. Outsourced activities may also be potential points for attack.

Another source of backdoors is the complicated organizational process for large insurers. Mergers and acquisitions are common. The result of this is that multiple different processes exist under the same roof—these are inconsistent and fragmented. The user identities and accesses may not be proper shape for quite some time following a merger. This leads to delay in execution and difference in levels of preparedness within the same organization. So although insurers do not take cyber security lightly, they are still prone to attacks.

Lack of discipline in implementing security patches and an ill-organized cyber security system forms more soft spots. Cyber drills may not be taken seriously, which results in lack of know-how when emergencies actually do come knocking.

16.5.5 Types of Threats

The threats can take the form of data breaches, security incident, privacy violation, phishing and skimming. Common tactics include: DDoS, snooping, phishing, ransomware, financial Trojan, CEO fraud, identity theft, malware, SQL injection, shell shock, advanced persistent threats, etc., (Business World USA 2017; KPMG 2017).

16.5.6 Impact

For a company in the business of hedging risk, being at risk to technology can be disruptive. A recent paper by the International Association of Insurance Supervisors lists the potential negative impacts on businesses as loss of confidential information leading to lawsuits, loss of reputation among clients, financial loss in the form of ransoms, recovery costs, ransom costs, fraud costs, hefty lawsuit payouts, disruption in business activities, destruction of physical infrastructure, regulatory pressure, impact on share price, etc. KPMG classifies these costs, in relation to time elapsed between their occurrence and the time when the incident was discovered, as immediate costs and slow-burn costs (KPMG 2017; Vegvizer 2018).

These risks are not to be taken lightly—estimates by some agencies say that the cost of cybercrime across different spheres of the economy will reach more than US$6 trillion per year, by the year 2021. The backdoors for cyber-criminals are open both from the internal side and through interactions of the insurers with external parties—what is therefore required is that foresighted insurers strengthen their game by addressing both internal and external issues pronto, if they wish to survive against the double whammy of cybercrime and technology-based competition.

16.6 Recommendations

We formulate a five-pronged strategy, in the context of the peculiarities of the insurance industry discussed above. This strategy is based on changes in the regulatory framework, collaboration among insurers, organization development, artificial intelligence-based security measures and cyber-physical systems-based security measures. These are discussed in more detail below.

16.6.1 Regulatory Framework

Given the highly collaborative nature of this industry, and for the protection of the rights of the unassuming end consumers who may get caught in the crossfire of the fallout from cyberattacks, regulators will definitely need to step up their game. The European Union has formulated stringent rules for the insurers with regard to data security and ownership, especially in the aftermath of the 2008 financial crisis which demonstrated that a flaw or fault in one organization was capable of bringing down the entire global economy like a pack of cards. Some of the areas in India that need a thorough revision with regard to regulation are:

- Responsibility assignment: after the attack.
- Data collection and ownership: before any attack.
- Cyber security guidelines: before any attack.

16.6.2 Collaboration

By the very nature of the business they run, insurers have multiple collaborations with various third parties. To ensure that fraud and cyberattacks do no propagate through the nexus of companies in the insurance value chain, blockchain and smart contracts can be explored more. Also, companies need to pool in resources and know-how to step up the research and development game by learning from each other's weaknesses. An international breach warning system would be an ideal development out of such collaboration.

16.6.3 Organizational Development

Insurance has been the ground of large players for decades now. Although tech-based insurance startups have been gaining ground in recent years, mergers and acquisitions are the norm which keeps the number of major players nearly constant. One of the issues that this throws up is complexity in the integration of processes belonging to the organizations which were merged. Thus, organization development and restructuring make even more sense in the face of cyber threats—to make processes consistent, information flow uninterrupted, and to eliminate any backdoors that may have been overlooked. Thus, what is needed in the organization are the following:

- Integration of diverse processes.
- Threat Intelligence Platform based on the cyber kill chain.
- Dedicated team for tackling cyber situations.
- Regular cyber security drills.
- Regular reminders about basics, like changing passwords.

The keywords are preparedness, awareness, capability and collaboration. CEOs will need to take up the leadership with regard to this organizational steering.

16.6.4 Artificial Intelligence and Machine Learning

As the age-old adage goes, it is always important to know your enemy. Lockheed Martin gives a good framework on how cyberattacks are usually executed, called the cyber kill chain (Lockheed Martin 2015). This framework is basically focused on intrusion-based attacks like malware. It may not be instantly applicable to other threat vectors like rogue insiders, social engineering, etc. (Fig. 16.3).

Machine learning algorithms are already heavily utilized by the insurance sector for detecting patterns of fraud. These can be exploited further for intrusion-based attacks for which pattern identification techniques are a common prediction and detection tactic, to make the entire security system of the insurance industry more robust.

In this task, the cyber kill chain is important for the structure it can provide to any attack recovery process. Also, simulations built on this kill chain can help identify potential backdoors that hackers can exploit. We suggest the following machine learning algorithms for predicting, preventing and detecting cyber incidents and attacks:

- Predict: Prediction requires assigning probabilities of occurrence to possible scenarios. Algorithms which can be used for this task include Markov models, Bayesian Belief Networks, etc.
- Prevent: This requires building up software-based, adapted security infrastructure. Deep learning can be utilized in encryption algorithms and firewalls to make them more resilient to creative and highly adaptive hackers.

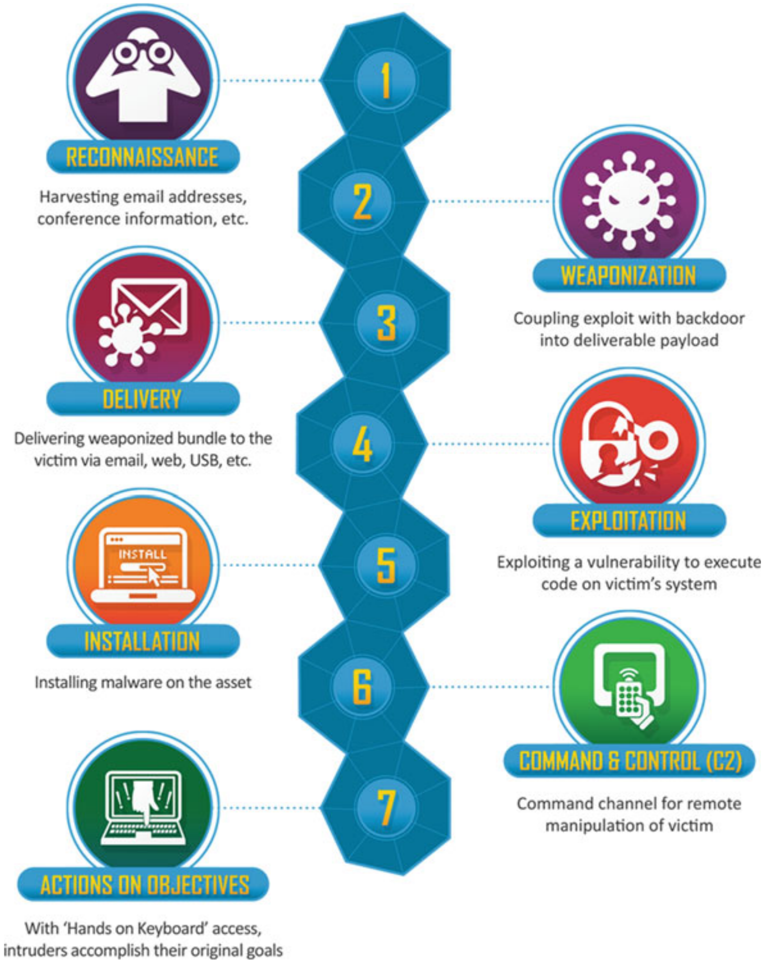

1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Fig. 16.3 Lockheed Martin's cyber kill chain®

- Detect: Detecting an attack needs identification of out-of-the-ordinary events taking place. For this task, fuzzy logic, classification and anomaly detection techniques are already being heavily utilized.

16.6.5 Cyber-Physical Systems

Many cyberattacks originate from rather unsophisticated places—like an infected pen drive inserted into a server containing sensitive data, social engineering employees, etc. So, hardware-based security measures will never lose their importance, however sophisticated the software security measures become. But more than just hardware infrastructure for security, we can look at utilizing “intelligent hardware.” It can take the form of:

- Track: through biometrics and mobile devices the activities listed offenders, employees.
- Sensors: biometrics, activity detection.

16.7 Limitations and Further Research

This research looks at organization development as one of the recommendations for streamlining internal processes and thus preventing cyberattacks. It does not state where specifically this change management methodology can be applied. This will require a case study and survey-based classification of organizations and identification of pain points.

Machine learning for predicting cyberattacks is a newly emerging area, which has plenty of questions to explore. It has the potential to spawn a new branch of study at the intersection of artificial intelligence, networking, cyber-physical systems and information theory.

16.8 Conclusion

Former Cisco CEO John Chambers is regarded as a visionary who has the ability to see technology and its impact much before that technology comes “in vogue” (Kerravala 2015). He described the situation regarding the impact of Internet, IoT, networking and the resulting cyber security threats rather succinctly as:

> There are two types of companies: those that have been hacked, and those who don’t know they have been hacked.

According to statistics released by the National Crime Records Bureau, cybercrimes and/or IT-related crimes have increased by nearly 150% from the year 2012 to the year 2014. It is a situation that needs to be considered extremely seriously as technology penetration becomes more entrenched across industries (Kumar 2017).

As the insurance industry becomes more tech-savvy in order to remain competitive and competent in the future, the nature of risk they face is evolving as well. Persistent, consistent and innovative efforts are perhaps the key attitude characteristics that any cyber incident handling team in the insurance industry will need to imbibe—as the attackers become more creative, the people on the other side will need to catch up as well.

References

BT Online. (2017, October 4). *Massive data breach hits 6,000 Indian organisations including govt offices, banks: Quick heal*. Retrieved from https://www.businesstoday.in/current/economy-politics/data-breach-hacker-data-of-6000-indian-businesses-for-sale-on-internet-quick-heal/story/261370.html.

Business World USA. (2017, December 1). *Cyber security risks facing insurance companies in 2017*. Retrieved from http://businessworld-usa.com/cyber-security-risks-facing-insurance-companies-2017/.

EY. (2017, October). *Global insurance trends analysis 1H 2017: Upside potential, side-ways risks*. Retrieved from http://www.ey.com/Publication/vwLUAssets/ey-global-insurance-trends-analysis-1h-2017/$FILE/ey-global-insurance-trends-analysis-1h-2017.pdf.

EY. (2010, September). *Indian insurance sector: Stepping into the next decade of growth*. Retrieved from http://www.ey.com/in/en/industries/financial-services/insurance/indian-insurance-sector.

Gooptu, B. (2017, October). *PolicyBazaar raises Rs 500 crore from IDG Ventures India and others*. Retrieved from https://economictimes.indiatimes.com/small-biz/money/policybazaar-gets-rs-500-crore/articleshow/61061383.cms?from=mdr.

IAIS. (2016, August). *Issue paper on cyber risk to the insurance sector*.

IBEF. (2018, March). *Indian insurance industry overview & market development analysis*. Retrieved from https://www.ibef.org/industry/insurance-sector-india.aspx.

IIF. (2016, September). *Innovation in insurance: How technology is changing the Industry*.

Kerravala, Z. (2015, July 24). *John Chambers' 10 most memorable quotes as Cisco CEO*. Retrieved from https://www.networkworld.com/article/2952184/cisco-subnet/john-chambers-10-most-memorable-quotes-as-cisco-ceo.html.

KPMG. (2017, January 25). *Facing the cyber threat in the insurance sector*. Retrieved from https://home.kpmg.com/qm/en/home/insights/2017/01/facing-the-cyber-threat-in-the-insurance-sector.html.

Kumar, M. (2017, January 26). *Cyber security: Insurance is critical in a digitised world*. Retrieved from http://www.financialexpress.com/economy/cyber-security-insurance-is-critical-in-a-digitised-world/522537/.

Lockheed Martin. (2015). *The cyber kill chain*. Retrieved from https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html.

Moynihan, S. (2018, January 12). *Who's the best target for cyber cover*? Retrieved from http://www.propertycasualty360.com/2018/01/12/whos-the-best-target-for-cyber-cover?slreturn=1518823098.

Sangwan, S. (2016, August 10). *10 promising home automation startups in India*. Retrieved from https://www.indianweb2.com/2016/08/10/10-promising-home-automation-startups-india/.

Singh, S. (2014, September 15). *Data theft threat sees rise in cyber security insurance policies*. Retrieved from http://indianexpress.com/article/india/india-others/data-theft-threat-sees-rise-in-cyber-security-insurance-policies/.

Vegvizer, T. (2018, January 29). *Cybersecurity threats in the insurance industry*. Retrieved from http://www.propertycasualty360.com/2018/01/29/cybersecurity-threats-in-the-insurance-industry.