MarketLine

Cybersecurity in Insurance

Digital wave demands insurers be vigilant

MarketLine Case Study

Report Code: ML00030-047
Published: August 2019

1. Overview

1.1. Catalyst

Cyber insurance cover (mainly liability-related) has been evolving for the last 10 years. Initially this product was oriented to meet developments in the telecom, media, and technology (TMT) industries. The type of coverage that once existed was privacy breach liability (a traditional risk transfer). It was developed as add-on cover or bundled with professional indemnity liability cover.

1.2. Summary

There has been a move away from a prevention-based approach to cyber-attacks towards active detection and timely responses to cyber-attacks. This approach factors in three levels of cybersecurity: people, process, and technology. Many chief information security officers (CISOs) and security executives are investing in detection and response-based technologies such as deception, endpoint detection and response, software defined segmentation, and behavior analytics.

Insurance carriers – like all other industries – should prepare for cyber-attacks by sharpening their capabilities. In particular, the insurance sector needs to instill governance, measures, and ongoing training of agents and insurance staff. At the same time they should leverage the start-of-the-art technology and defense techniques offered by cybersecurity vendors. The impact of cybersecurity is rising in severity of threat and response needed to combat it. As insurers grapple with managing the growing number of digital-related risks, it should be emphasized that getting onto the front foot in terms of cybersecurity does not just mean layering IT systems on top of legacy solutions. Rather, an approach that involves a mix of people, processes, and technology is required to drive a cyber-resilient enterprise. The relevance of cybersecurity to insurance now extends across a wide-range of products. Connected cars and usage-based insurance (UBI) offer benefits for insurers such as more accurate segmentation of risk profiles and more efficient claims handling capabilities.

Determining pricing models for cyber insurance and modeling cybersecurity risks have been major hindrances for actuaries, underwriters, and insurance providers. The difficulty in modeling risks associated with cyber threats in commercial lines of insurance products has opened up opportunities to a growing number of start-ups that offer security benchmarking to help insurers limit liabilities and forecast losses.

Growing global regulatory concerns about the loss of personally identifiable information, the cost of handling breaches (including the cost of reporting breaches to regulators, customer regulation, PR costs, and legal expenses), increasing awareness of cyber risks, and the growing number of cyber-attacks have seen cyber insurance expand beyond TMT.

Table of Contents

2. Need for adaptation of cybersecurity to new threats is strong

Insurance carriers – like all other industries – should prepare for cyber-attacks by sharpening their capabilities. In particular, the insurance sector needs to instill governance, measures, and ongoing training of agents and insurance staff. At the same time they should leverage the state-of-the-art technology and defense techniques offered by cybersecurity vendors. The impact of cybersecurity is rising in severity and a strong response is needed to combat it.

2.1. Cybersecurity is having growing influence on insurance

As insurers grapple with managing the growing number of digital-related risks, it should be emphasized that getting onto the front foot in terms of cybersecurity does not just mean layering IT systems on top of legacy solutions. Rather, an approach that involves a mix of people, processes, and technology is required to drive a cyber-resilient enterprise. Cybersecurity has always been viewed as a technology risk rather than a business risk. This misconception extends to business resilience, which is usually thought of as disaster recovery among insurance CISOs and security executives.

In the meantime, insurance carriers and their associates are gearing up for the stringent regulatory scrutiny that will accompany GDPR, which came into effect in May 2018. They are aware of their overall accountability to recognize cyber threats in advance, reduce an organization's exposure to malicious attack and, most importantly, react quickly. In practical terms this requires insurers to put in place and follow through on a watertight cybersecurity strategy.

2.1.1. Traditional models are unable to cope with challenging demands now placed upon them

In today's digital world the boundaries of insurance have extended beyond the enterprise, as insurers increasingly co-operate in new ecosystems built around managing newly digitized assets. These include connected cars, healthcare monitoring, and connected homes. The ecosystems comprise healthcare providers, utilities companies, maintenance services, manufacturers, service delivery agents, medical billers, and other commercial partners such as fintechs and insurtechs. In these contexts, efficient operation requires dedicated customer data to flow efficiently from outside to inside the insurer's enterprise defense fence. In this new world order, the risk landscape becomes unbounded. The practice of relying only on traditional security and risk management models is obsolete. Traditional approaches to protection originated in a world where organizations owned most of their data assets. Technology presents a powerful potential opportunity to insurers, creating a flexible environment where new products and services are rolled out with improved customer relationships. In parallel, security is expected to top up insurers' investment agenda; managed security providers in particular should help cyber risk mitigation.

2.1.2. Watertight security for fleet data is essential now new technology is entering the mass market

Connected cars and usage-based insurance (UBI) offer benefits for insurers such as more accurate segmentation of risk profiles and more efficient claims handling capabilities. While there remain concerns about data privacy, customers have become more open to the idea of sharing their data with their insurer in exchange for discounted premiums or additional services.

According to the NAIC, UBI is expected to grow by 36% by 2020 (the proof of concept has been tested, and many insurers have already deployed telematics solutions and associated policies). The largest markets for telematics insurance are, in

order, the US, Italy, and the UK. This trend has also begun to spread slowly to Asia, with global French insurer AXA Inc. launching the first UBI product in Southeast Asia. It is not all good news for insurers, however. These telematics solutions generate a massive volume of sensitive personal and operational data that must be secured. Under GDPR, for instance, insurers, data processers, and controllers will be held responsible for any data breaches. This also requires insurers to be vigilant in choosing their telematics ecosystem partners. Insurers will prefer vendors that have a strong portfolio, including high standards of built-in security, capabilities, and advanced technology with strong strategic alliances.

2.2. Lack of access control presents insider threats

Lack of accountability and the management of privileged user access are among the biggest challenges. Insurers frequently suffer from either unrealistic policies (resulting in them being bypassed because of a lack of resources) or having no protocols. This is particularly apparent in relation to off-boarding staff or contractors' processes. Identity management vendors can help here by automating the process of removing the access rights of off-boarded employees. The International Association of Insurance Supervisors reported that insurers do not understand the concept of efficient internal process monitoring. The association referred to several cybersecurity incidents in the sector that resulted from the absence of proper internal controls. For instance, a 2012 fraud case within a French mutual insurance company resulted from internal data theft from a replicated environment that contained sensitive client information; this led to identity theft and a number of fraudulent claims.

Privileged identity management frequently meets with technological roadblocks such as regular changing of networks with heterogeneous hardware and software platforms, usually comprising a mix of new and legacy in-house components in which privileged credentials are stored in different ways. The implementation of identity management processes requires a high level of culture change. The focus should be first on the process; technology by default will be part of the change process. Considering that individuals who once enjoyed unlimited, anonymous access will likely resist the change, it makes sense that the project is only likely to succeed with active support from top management. Insufficient control over user accounts and access rights is a major problem for insurers, highlighting the necessity of introducing appropriate discipline into the process.

2.3. Legacy systems pose a higher security risk

Insurance carriers are fully aware that their security posture must be responsive and agile to counter the growing cyber threat. Equally they feel that the effectiveness of their defenses is constrained by a range of factors, such as IT legacy systems. Outdated systems remain a source of underlying vulnerability for both insurers' networks and the sensitive data that resides in them. Because some carriers cannot identify where some of their data resides as they have expanded through acquisitive activities, legacy systems accumulated from the purchased companies with heterogeneous IT systems pose a major cyber risk. In security terms, capabilities are fragmented and decentralized, generating substantial control challenges. Replacing legacy software across the enterprise can be cost-prohibitive, considering the disruption this would cause to daily routine. But cyber-attacks can have far-reaching financial and reputational ramifications. According to a recent survey by Capgemini, almost half of insurers do not patch their systems in a timely fashion.

Managing vulnerabilities on critical systems should be prioritized by insurers to prevent exploitation attempts by attackers. The timely application of patches is essential to outmaneuver known threats. For example, WannaCry could have been prevented if the affected systems had been patched. Patch management therefore should be guided by a formal policy and documentation. On all counts, ring-fenced commitment from senior management is needed to support better patching management control.

Some legacy systems are critical to an insurer's business, but the operation of these systems requires careful consideration. Vendors no longer support these systems. Network segmentation vendors can help in isolating the enterprise network, allowing legacy systems to reside in their own subnets.

3. Changing nature of cyber threats raises numerous challenges

The extent of threat that now exists and the international responses to them are many and varied. New laws and regulations are being created around the world, but so far no single set of ideas has emerged. Threats are gathering strength. Examples of malware and other means of attacking computer systems have gained worldwide notoriety, focusing attentions on the potential consequences of a successful cyberattack the necessity of getting protections correct.

3.1. Threats are gathering in strength, forcing cybersecurity to meet greater challenges

Cyber insurance cover (mainly liability-related) has been evolving for the last 10 years. Initially this product was oriented to meet developments in the telecom, media, and technology (TMT) industries. The type of coverage that once existed was privacy breach liability (a traditional risk transfer). It was developed as add-on cover or bundled with professional indemnity liability cover. However, growing global regulatory concerns about the loss of personally identifiable information, the cost of handling breaches (including the cost of reporting breaches to regulators, customer regulation, PR costs, and legal expenses), increasing awareness of cyber risks, and the growing number of cyber-attacks have seen cyber insurance expand beyond TMT.

The cyber insurance market is set to grow quickly to meet emerging demand for cover on the liability and property sides. According to Aon, the cyber insurance market achieved 30% annual growth between 2011 and 2015. In the US, cyber insurance generated around $1bn in direct written premiums in 2015. AIG, Chubb, and XL Group led the market in 2015 with market shares of 22%, 12%, and 11% respectively. The US cyber insurance market has potential to grow to $5bn by 2018 and $7.5bn by 2020. Yet the insurance industry is currently struggling to provide more granular policies to fit all businesses and cover different types of cyber risk. In part this is due to the lack of historical data on cyber incidences, as well as the lack of standardization when it comes to industry terminology.

3.2. Emerging needs are shifting cyber insurance to solutions, helping start-ups grow

Insurers have been selling cyber insurance coverage for some time, but these coverages are limited—usually revolving around data breaches and loss. Since 2015 we have witnessed an upward trend in insurers looking to expand the cyber insurance market and cover new cyber risks, such as protecting digital assets and business interruptions caused by cyber-attack. However, cyber insurers need to improve their understanding of the new cyber risks in order to improve risk modeling, pricing, and reserving decisions. In that context we see two emerging trends in cyber insurance. Firstly, to accelerate their progress in improving the reliability and accuracy of risk modeling, loss forecasting, and capital reserve allocations, insurers have begun and will continue to seek help from vendors and partner up with cybersecurity start-ups, as they realize they will not succeed by going it alone.

According to Verizon Data Breach Investigation (2016) around 77% of breaches fall within the insider and privilege misuse category. This is caused by an internal party/individual, which could be a dissatisfied employee who leaks data on purpose or careless staff who unintentionally disclose sensitive data. If anything this could be an indication of a lack of appropriate cybersecurity measures within an organization. Organizations are increasingly looking to restricting access to company-sensitive and key accounts, as well as assigning special account access privileges to authorized individuals.

Many organizations have started to offer cybersecurity education and training to employees and staff. Insider breaches are problematic: 48% of insurers surveyed by Accenture reported experiencing malicious insider threats, while 55% lacked confidence in their internal security monitoring. Insurers will look to track the data flow in all IT systems, applications, and components.

Determining pricing models for cyber insurance and modeling cybersecurity risks have been major hindrances for actuaries, underwriters, and insurance providers. The difficulty in modeling risks associated with cyber threats in commercial lines of insurance products has opened up opportunities to a growing number of start-ups that offer security benchmarking to help insurers limit liabilities and forecast losses. To give an example, Bisight helps insurers understand the security weaknesses of their potential and existing clients. These nimble players offer direct expertise and resources to quantify risk and an operational platform for insurance providers. The growth in such start-ups owes much to substantial funding from major venture capital firms such as Sequoia Capital, New Enterprise Associates, and Index Ventures. This is expected to attract the attention of leading cyber insurance operators, which will look to collaborate in the form of acquisitions or strategic partnerships in order to leverage start-ups' technical knowledge and thereby strengthen their offerings.

3.3. Organized crime online is a growing problem for cybersecurity efforts

Increasingly, more sophisticated hacking has been perpetrated by groups of hackers against governments, nations, and states rather than a single individual. Anonymous and Lulz Security are two of the most widely known groups. They use sophisticated hacking methods to bring down large institutions via DDoS attacks that temporarily eliminate the availability of web or email servers. Anonymous – in alliance with Ghost Squad Attackers – claims to have brought down several central banks in this way, including the Bank of Greece, the Federal Reserve Bank of Boston, the Bank of England, and the Bank of France. The group also claims to have brought down the London Stock Exchange for over two hours in early June 2017.

Online fraud is on the rise on the back of technology cycles such as P2P lending, mobile banking, e-commerce, and the IoT. Social media encourages the reckless dissemination of personal information on the web, which facilitates identity theft. Moreover, hackers have access to low-cost tools and methodologies on the internet and little prospect of being caught. As more personal data ends up stored in the databases of internet companies, specialist data resellers can create more and more big data algorithms that dice and slice this data for resale. Credit profilers such as Experian and Equifax are one set of beneficiaries. Online fraud detection companies such as IBM, Guardian Analytics, RSA (Dell/EMC), and Kount are another.

4. Cybersecurity technologies are evolving at speed

There has been a move away from a prevention-based approach to cyber-attacks towards active detection and timely responses to cyber-attacks. This approach factors in three levels of cybersecurity: people, process, and technology. The prevention approach is futile unless it is combined with detection and rapid response approaches. However, combating an inside threat for companies remains very difficult. Major retail companies are playing an enlarged role in the field of cybersecurity, revealing the extent of threats that are now commonplace.

4.1. Active protection now trumps prevention-based approaches

Many chief information security officers (CISOs) and security executives are investing in detection and response-based technologies such as deception, endpoint detection and response, software defined segmentation, and behavior analytics. CISO and security executives are looking to achieve and optimize visibility across their infrastructure to ensure an adequate protection from security incidents.

Corporate expenditure on cybersecurity has been slapdash over the past two years. Multiple vendors have sold a patchwork of security products without considering how well they work together. The result has been a lack of strategic direction and co-ordination within many companies' IT departments. At the top of the chain could be unified threat management systems powered by intelligence engines that take a risk-based approach to security. By automating threat discovery, investigation, and response, unified threat management can reduce incident response times and enhance overall threat detection rates. The leading companies in unified threat management are Check Point Software, Fortinet, IBM, SecureWorks, Sophos, and WatchGuard.

However, some breaches are due to insider threats – whether through malicious intent or negligence – so behavioral analytics are critically important as a cyber defense. AI leaders IBM, Google, Microsoft, Splunk, and Palantir are among the best placed to exploit this trend. But there are also a number of start-ups specializing in behavioral analytics in the cybersecurity sector, including Cloudera, Bay Dynamics, Carbon Black, E8 Security, and Securonix.

4.2. Large consumer companies are at forefront of cybersecurity development

Amazon and Mastercard are among the first major payment players to use selfies as an alternative to security passwords. In October 2016, Mastercard announced the European rollout of Identity Check Mobile, a new payment technology application that uses biometrics (e.g. fingerprints or facial recognition) to verify a card holder's identity. Passwords offer poor security for most digital transactions, and the time to replace them is overdue. Facial recognition and fingerprint technology companies should be a major beneficiary of this trend. Leaders here include Clarifai, 3M Cogent, and Safran.

British telecom operator TalkTalk was fined £400,000 for security failings by the Information Commissioner's Office in the aftermath of its October 2015 cyber-attack, and. There is a growing market for post-breach strategy consultancy services. Post-breach strategy focuses on gathering information about the cyber-attack as quickly as possible after the event and formulating a credible PR strategy to demonstrate that management remain in control of their business and have taken all actions possible to protect critical digital assets. The leading post-breach consultancy services companies include IBM, Accenture, KPMG, PwC, FireEye, Herjavec Group, and root9B.

Few organizations have the skills base to build cybersecurity defenses themselves or even make effective use of cybersecurity technology. This tilts the balance in favor of managed security services, whereby a single security vendor manages an organization's cloud applications, compliance with data protection laws, and other cybersecurity risks. Leaders in managed security services include IBM, Symantec, SecureWorks, WIPRO, BAE Systems, HP Enterprise and Trustwave (SingTel). Telcos like AT&T, BT, CenturyLink, NTT, Orange, and Verizon also operate in the space.

5. Appendix

5.1. Further reading

Business intelligence technology: Opportunities present but challenges must be overcome - Case Studies published by MarketLine

ICT Investment Trends in the UK: Data protection and recovery form the core of enterprises' IT investment strategies - Case Studies published by MarketLine

6. Ask the analyst

We hope that the data and analysis in this case study will help you make informed and imaginative business decisions. If you have any questions or further requirements, MarketLine's research team may be able to help you. The MarketLine Research team can be contacted at ReachUs@MarketLine.com.

7. About MarketLine

At MarketLine, we deliver accurate, up-to-date insights on over 100,000 companies, 3,500 industries, 215 countries, and 3,000 cities as well as the latest news and financial deal information from within your market and across the globe.

Established in 1997 when the Internet was in its infancy, we recognized the need for a convenient and reliable data service to help our clients understand local and global markets and the companies operating within them.

In today's information-rich world, sifting fact from fiction to pick out what's relevant and what's up to date has become the new 'holy grail' in business information provision.

Hundreds of dedicated research professionals aggregate, analyze, and cross-check facts in line with our strict research methodology, ensuring a constant stream of new and accurate information is added to MarketLine every day.