IIMC Library Clipping Service | Source: News: Online: Forbes India | Dated: 25-01-2022

Will insurance improve cyber-security practice for businesses?

Cyber-insurance is a convenient and necessary CRM tool for improving business security practices, whose multi-stakeholder market needs far better regulation than the status quo

BY RANJAN PAL, BODHIBRATA NAG AND CHARLES LIGHT

Apart from providing loss coverage as its salient functionality, cyber-insurance carries with it the essential additional promise of improving cybersecurity

Is cyber-insurance even necessary for today's businesses in the first place?

One could argue first-up that deploying advancements in the last decade of security-improving technology is sufficient for IT-driven businesses to secure their service operations efficiently. Sadly enough, this is not the case, with many of these businesses that drive digital (IoT-propelled smart) societies not deploying robust cyber-security solutions (either in quality and/or in the manner of use) that should necessarily complement the modern IT infrastructures they own to provide critical and day-to-day services. This fact gets repeatedly confirmed in annual surveys by popular CRMaaS firms (for example, Advisen, EY, PartnerRe, Deloitte). It is not surprising that as a result, most industries around the globe—small, medium, or big, are

successfully breached every year through malicious events that include cyber-extortion (for example, ransomware), unintentional data disclosures, lost or stolen data, data breaches, unauthorised data collection and disclosure, identity theft, network/website disruption, business email compromise via social engineering, and denial of service.

An obvious question to ask here is: why are businesses not investing enough in cyber-security technology? We attribute the following facets of an answer to this question:

(i) Despite the rising trend in the last few years (thanks to significant cyber-breaches such as the Mirai DDoS and the WannaCry/Petya ransomware attacks) among corporate boards acknowledging cyber-risk to be a top-five concern for business continuity, reputation, and profitability; the proportional time, resources, and effort have not been put in to design effective board-level policies/nudges that aptly incentivize employees to behaviourally improve their cybersecurity practices, and make the best use of installed security products.

(ii) Cybersecurity technology solutions are a market for lemons (a term coined by economist George Akerlof in 1970). The root of the technology efficacy problem is primarily economically driven by information asymmetry between the parties that prevent technology buyers (for example, the CISOs and the enterprise team of organisations) from effectively evaluating technology, and incentivising security vendors to sell sub-optimal solutions in the market, that are not as effective as promised and which reduce trust in cybersecurity technology. More specifically, the technology solutions market is too congested with tons of products for buyers to give in quality time and effort to evaluate and rank the effectiveness of each product—to the extent that the buyers believe that lack of quality is the reason behind too many products to existing concurrently in the market.

(iii) Cybersecurity products are often an outcome of a high-risk "casino economy" where a fragmented vendor industry is configured to manufacture products they think (a) venture capitalists will invest in, (b) that larger companies might want to integrate and make the smaller companies follow suit, and (c) that customers can be convinced to buy. These products, akin to a gamble, might be innovative enough to help cybersecurity occasionally, or they might not, but frankly, nobody has a clue. Now iterate this process over 10-15 years, and you end with a lot of complexity, layers of obsolete and often non-performing technology that requires ever more scarce human expertise to maintain and keep running.

(iv) IoT has ushered in a whole new and difficult challenge to manage cyber-risk in modern IoT societies technologically. Billions of (cheap) IoT devices (currently, tens of billions, and projected by Cisco to be a whopping 125 billion by 2030) are deployed in most industrial sectors and wirelessly connected as part of intra- and inter-organisation networks. Most of these devices are unattended for long periods, have poor security features due to limited processing and

memory capabilities—incapable of running sophisticated security tools even if desired, and significantly enough is loaded with weak default passwords. This has made Industrial IoT-driven cyber-physical industry systems relatively easy to be breached, as evident from the catastrophic Mirai botnet attack a few years ago. The denser the IoT penetration, the greater the likelihood of system and systemic cyber risk, and consequently, the more significant the negative social and economic impact.

In summary, there is a severe lack of C-suite endorsed CRMaaS solutions that (a) either aptly nudge employees to inculcate good cyber-hygiene and or transfer the liability to the employees for their (mis) behavioural security practices—especially in the WFH age; and (b) unaffected by the market inefficiency of the cyber-security product's economy. These two factors combined make it virtually impossible for businesses to not only be cyber-risk-free but also not be a potential target for cyber-breach risks of modest strengths. Simply put, companies necessarily need to resort to third-party residual cyber-risk mitigation services such as cyber-insurance to cover the first party and, more importantly (cascading) third party losses.

Why is the cyber-insurance economy so inefficient despite rising demand?

It is pretty intuitive in principle that realising dense cyber-insurance markets in practice can enable enhanced cyber-security. This is simply because dense markets will induce a premium pricing mechanism that will appropriately transfer cyber-risk liability upon the businesses and subsequently their employees—leading to better adopted cyber-security practices, at the same time will reduce market inefficiencies in the security product economy. The big two-pronged question then stands: is the current global cyber-insurance economy dense and efficient enough?

According to worldwide empirical data collected by major (consulting) firms in recent years (Deloitte, Fitch, Advisen, FERMA), more IT-driven organisations (ITOs) today, more than ever, carry cyber insurance—with 80 percent of organisations in the USA currently investing in cyber-insurance products. Nearly 55 percent of organisations in North America and Europe in sectors spanning health, energy, transportation, finance, and retail are buying stand-alone cyber-insurance policies, with the global average in this category being only 26 percent. There are at least 300 commercial cyber-insurance vendors around the world, in an annual market that is worth approximately $8 billion globally (projected to grow to $25 billion by 2025)—ransomware represents the number-one cause of loss claims by businesses today, with the average ransom rising to $247,000 and the average incident cost up to $352,000 (as of 2021). This (C-suite promoted) take-up rate for cyber insurance has steadily climbed since 2011 (thanks again to the fear factor multiple attacks that became a threat to the customer-facing trust and reputation of service-providing ITOs) when just 34 percent of ITOs in the USA and Europe bought some cyber coverage in a global market that was hardly worth half a billion USD. Add to

this the current push from the legal and policy front in certain parts of the world to invest in cyber insurance. For example, in February 2020, the Californian assembly introduced a bill to make cyber insurance mandatory to process regulated and protected personal information for all state contractors. The rise in data privacy laws, such as the Personally Identifiable Information (PII) and the Health Insurance Portability and Accountability Act (HIPAA), in the US; the global standard, Payment Card Industry- Data Security Standard (PCI-DSS); and the European Union's (EU) General Data Protection Regulation (GDPR) are persuading insurance providers to focus on cyber insurance measures. In February 2020, the European Insurance and Occupational Pensions Authority (EIOPA) released its strategies for cyber underwriting and supervisory technology to build a solid cyber insurance market. EIOPA will work with national authorities to ensure periodic assessment and supervision of cyber underwriting and risk management practices in Europe. According to Willis Tower Watson's Insurance-Linked Securities (ILS) report, in October 2018, the government of Singapore introduced a commercial cyber risk pool to provide corporate buyers in Asia with cyber insurance, along with ILS. It seems that cyber-insurance markets around the globe are chugging along, catalysed through commercial, legal, and policy initiatives.

However, the not-so-good news is that despite the rising popularity and market base for cyber-insurance, the supply-demand gap today is enormous—in other words, the global cyber-insurance market is highly sparse. According to McAfee, the value of cyber-loss around the globe annually amounts to approximately $450 billion, whereas the annual cyber-insurance market is worth at most $8 billion globally. Even if one reserves an optimistic upper cap of $250 billion organisation expenditure in security vendor products, there is a gaping $200 billion hole in residual cyber-risk impact, out of which only $8 billion gets plugged. Surprisingly enough, despite all the visionary promises of cyber insurance, corporations do not seem to be behaving rationally when it comes to investing in cyber-insurance products. More specifically, market data suggests that cyber-insurance policy buyers feel the following emotions that go against them buying stand-alone products: the price is too high, the coverage is too low, not satisfied with prior service, very restrictive, and often unclear coverage terms, and prefer self-insurance options. The market statistics clearly show that the supply-demand dynamics are not well matched and reflect the observed insurance market inefficiency. The main question that then arises is: what are the underlying causes of such inefficiencies?

We identify three crucial and modern causes (some unsurmountable in the near run) that unfortunately prevent society from harnessing the immense cyber-security improving the potential of cyber-insurance products:

(i) Information asymmetry (in the form of moral hazard and adverse selection) between profit-minded risk-averse insurers and the insured organisations has led to cyber-insurance solutions

being sold in a market of lemons, similar to that of cybersecurity technology solutions. The existence of moral hazard on the side of the insured's preventing cyber-insurers from selling contracts to all who demand, and that too without substantial coverage (resulting in large deductibles) and/or with waiting periods, in many cases where coverage policies are sold. In the absence of mandatory cyber insurance, such weak and often unfairly-priced policies strongly discourage firms from buying them. The standard adverse selection problem in traditional insurance is even more pronounced in the case of cyber-insurance, simply because of (a) the intricate complexity of a large cyber-network of service inter-dependent organisations that make it extremely difficult for insurers to have all the required information needed to estimate cyber-risk accurately—significantly more so in the Covid-19 age with employees going remote, and (b) the lack of enough robust, transparent, and globally universal cyber-information disclosure laws that prevent organisations, and nation-states from releasing cyber breach/posture information to the needed extent that allows strong data analytic engines to compute the fair price of insurance contracts—thereby improving market density. Information asymmetry challenges are the main reason that cyber-insurance product markets are inefficient.

(ii) Network externalities induced by the omnipresence of software vulnerabilities in a few operating systems (OSs), application programs, and security products, but those that are commonly used by most IT systems around the world result in correlated cyber-risk threats of significant amounts to the coverage dislike of risk-averse insurers. The likelihood of such statistically non-independent risks increases multi-fold in the current IoT age where billions of devices with poor cybersecurity postures (for example, default passwords, un-encrypted firmware access, unauthorised backdoor access, lack of use of Secure Socket Layer (SSL) technology to connect IoT to the cloud) are associated with one another to the drooling delight of cyber-hackers ever-ready to launch simple attacks that result in cascading catastrophes (such as in the case of Mirai and WannaCry cyber-attacks), leave alone the need for sophisticated ones. Such environments result in aggregated cyber-risk from multiple dependent and correlated source points in a network and is a pain-point for cyber-insurance firms that needs to bear the liability for cascading aggregated cyber-risk—more so when recent scientific research has mathematically proven that covering such aggregate cyber-risks is infeasible for profit-minded insurers. This will likely result in insurance companies being ultra-cautious in underwriting and selling enough policies for the social good. Though it is a commonly known fact that the cyber-insurance industry is aware and present a market about the potential aggregation risk in cloud computing services, such as Amazon Web Services (AWS) and Microsoft Azure; however, given the layers of security, redundancy, and 38+ global availability zones built into AWS, it is not necessarily the easiest target for adversaries to cause a catastrophic event for insurers in the first place. There are potentially several hundred systemically important vendors (for example, DNS providers, websites) that could be susceptible to concurrent and substantial business interruption and may not have the kind of security that exists within providers like AWS.

Insurance firms may not be ready yet to sell attractive coverage policies for such businesses.

(iii) Computational limits will prevent optimal cyber-insurance underwriting in the IoT era. To specify in more detail, the above-mentioned information asymmetry problem that contributes to the market for lemons induces a cost, commonly known as the lemon cost, that is usually kept within reasonable bounds in practice via the use of financial derivative contracts. Here, lemons are the insurance policy buying organisations that have a high-risk cyber-posture, but due to the lack of solid information disclosure policies in operation, they manage to hide their cyber-posture information from their insurers who get trapped into adverse selection. The lower the lemon cost, the more profitable the cyber-insurance business. In the best case, if a fully rational (computationally unbounded) cyber-insurer had a robust estimate of the number of lemons, it could enumerate over all combinations of their inclusion to verify that a certain threshold of lemons does not simultaneously file claims in a coverage package, thus bounding the lemon cost. However, for a real-life cyber-insurer who is computationally bounded, this enumeration is computationally infeasible. These enumeration problems are equivalent to variations of the so-called hidden dense subgraph problem, which theoretical computer scientists believe to be computationally intractable, even a computer cannot enumerate all possibilities in a reasonable amount of time. The bottom line is that under computational limitations, the lemon cost for cyber-insurers is amplified using a derivative structure, leave alone the latter's promise to ameliorate—a vital cause for cyber-insurers to shrink market sizes.

In summary, cyber-insurance markets today are just realising the tip of the iceberg of their potential in terms of improving security in cyber-space, simply due to the lack of market density and market inefficiency.

How can we boost cyber-insurance market density for improved cyber-security?

The dichotomy in cyber-insurance market survey statistics (source: Hiscox, Advisen) is the fact that non-buyers in the big SMB category are skeptical—at the same time, they are risk-averse enough for around 50 percent of them wanting to invest in cyber-insurance in the next two years. So a central question of interest here is: how can the current cyber-insurance business convert skeptical buyers into optimistic policyholders? There is a one-one correspondence between improved cyber-insurance market density and enhanced cyber-security. We provide five suggestions as possible answers to this question.

(i) The cyber-insurance business needs to re-think its existing pricing strategies. One way forward will be for insurers, agents, and brokers to address issues of affordability and coverage limitations that seem to be an obstacle to purchasing. The market needs to go beyond its currently prevalent 'more art than science' approach to price contracts based on subjective measures (what competitors are doing) to differentiate cyber-risk among organisations (source:

Advisen 2019 Cyber Risk Conference) and use data-driven actuarially sound probabilistic models to price contracts. The evolving nature of cyber-risk (novel attack and cyber-threat vectors, catastrophic cascading risk settings) may also be a barrier to the 'optimal' pricing of contracts. As a result, cyber-insurers are warned that they cannot simply afford to, be myopic, increase market density (and beat competition) by lowering prices or offering more (attractive) coverage for the same premium, as they might risk paying a steep price down the road. Such decisions should necessarily take into account the potential long-term impact of evolving exposures and third-party loss scenarios.

(ii) A cyber-insurance package should bundle value-added services. Rather than trying to 'beat' market competition only by reducing premiums and expanding on coverage, cyber-insurers should add customer value to their packages by bundling cybersecurity support to mitigate cyber-attacks. Recent market surveys (source: Advisen, Deloitte, FERMA) have shown that SMBs prefer holistic CRM services that include cyber incident response, cyber-posture assessment, crisis management, forensics support, and loss control advice and training as part of their cyber-insurance package. More specifically, to increase demand in addition to being market competitive, cyber-insurers could provide premium discounts to buyers who purchase a bundled package when compared to otherwise. There already exist such practices—for example, Marsh is partnering with multiple insurers to help clients pick effective cybersecurity products and services, while CNA Hardy has launched a series of partnerships to offer cybersecurity legal support and crisis management.

(iii) Policy buyers should be better educated about cyber-risks and appropriate policies. Insurers should educate less experienced policy buyers and those lucky enough not to have been majorly compromised by serious cyber-attacks, warning them about taking serious cognizance of the rapidly increasing probability of cyber-breach occurrence. Another important lesson for cyber-insurance firms to convey to buyers with low coverage through standard policies is that they cannot take it for granted that with an increasing cyber-attack rate on average, these policies will provide adequate cyber coverage and that these buyers should invest in stand-alone cyber-insurance policies (like they do for D&O or EPLI) where applicable. This, more specifically when over the last few years, many standard policy selling insurers have tried to 'bypass' cyber claims (especially when they are pretty significant), following (still ongoing) claims disputes over "silent" coverage policies with no clear terms of cyber-risk coverage, their causes, and their limits (mostly policies where cyber isn't explicitly named in a policy but isn't explicitly excluded either). A prominent example of this latter scenario is the cyber-insurance coverage situation post the NotPetya cyber-attack.

(iv) Government/Regulator policies should enforce clarity of cyber-coverage. Public policy and regulation should prescribe/lay down rules on what type of insurance policy should cover which types of cyber-risks. As an example, several countries (including Brazil, Chile, Colombia, Japan, Russia, and European Union members) have legislation or regulation that mandate a clear definition of what is included and excluded in a given policy. As another example, the Prudential Regulation Authority (PRA) in the UK issued a supervisory statement in 2017 outlining its expectations concerning the management of cyber insurance underwriting risk—clearly suggesting that companies should either offer explicit cover for cyber threats or introduce

robust wording exclusions for those risks.

(v) Collective information sharing between insurance market stakeholders should improve. Trusted, secure, AI-driven, and scalable cyber information (for example, regarding cyber-threats) sharing needs to be a foundational platform on which the cyber-insurance market stakeholders can rely. This would help reduce information asymmetry in such markets, build mutual trust among the stakeholders, improve premium pricing, and increase transparency in collaborative investigations to detect and deter threat actors. Inevitable regulatory policy barriers to jurisdictional collaboration on tracking cyber-threat actors should be reduced.

Ranjan Pal, University of Michigan Ann Arbor, USA
Bodhibrata Nag, Indian Institute of Management Calcutta, India
Carl Landhewr, University of Michigan Ann Arbor, USA
Jon Crowcroft, University of Cambridge, UK
Ed Hua, MITRE Labs, USA
Tathagata Bandyopadhyay, Indian Institute of Management Ahmedabad, India

Source: https://www.forbesindia.com/article/iim-calcutta/will-insurance-improve-cybersecurity-practice-for-businesses/73157/1