Interested in learning more about security?

SANS Institute InfoSec Reading Room

Cyber Insurance Conundrum: Using CIS Critical Security Controls for Underwriting Cyber Risk

There has been a number of insurance industry- related research done to define new cyber security frameworks to help insurers underwrite cyber risk. This research includes copula-based actuarial models for pricing cyber insurance based on the number of computers; using peaks-over-threshold method (from extreme value theory) to identifying "cyber risks of daily life"; using Principal-Agent model (from microeconomic theory); creating methodology for common cyber risk categorization; modeling cyber risk based on...

Cyber Insurance Conundrum: Using CIS Critical Security Controls for Underwriting Cyber Risk

GIAC (GLEG) Gold Certification

Author: Oleg Bogomolniy, oleg.bogomolniy@gmail.com
Advisor: Chris Walker
Accepted: 1/27/2017

Abstract

There has been a number of insurance industry- related research done to define new cyber security frameworks to help insurers underwrite cyber risk. This research includes copula-based actuarial models for pricing cyber insurance based on the number of computers; using peaks-over-threshold method (from extreme value theory) to identifying "cyber risks of daily life"; using Principal-Agent model (from microeconomic theory); creating methodology for common cyber risk categorization; modeling cyber risk based on operational risk, and more. However, there has been little to no input or research into cyber insurance related topics from cyber security experts. The purpose of this exploratory study is to propose the integration of a risk framework for underwriting cyber risk. This paper will analyze how CIS Critical Security Controls, along with its accompanying quantified metrics, benchmarking, and auditing tools can be used as a rating mechanism for determining the cybersecurity posture of insured organizations. Furthermore, such mechanism can be perpetually used for either self-assessments by insured organizations, or by independent qualified security assessors.

1. Introduction

During the past two decades, there has been an enormous wave of technological sophistication attributed to the proliferation and commercialization of the Internet. It appears in a blink of an eye the world became embedded in mobile technologies, entrusted to self-driving cars, consumed by the Internet of Things, and surrounded by flying drones delivering online orders from the sky. It is now evident that today's innovations may rapidly become tomorrow's common commodity - putting a tremendous pressure on the technology sector to minimize the innovation's speed to market, leaving little time for assuring adequate security (Krebs, 2016). In this context, it has been abundantly debated whether achieving 100% security is technically possible or economically necessary. Meanwhile, IT risk managers succumb to a dilemma of how much cyber risk should be retained, mitigated, or transferred to a third party. While different options and methods exist for transferring cyber risk to a third party, this paper focuses on the means of transferring a portion of the financial cost associated with a cyber incident to an insurer (i.e. cyber insurance policy) in return for a fee (i.e. insurance premium), henceforward, the term referred to as, cyber insurance.

Much of academic research and studies related to the cyber insurance industry has been conducted over the past two decades to understand its merits and demerits. Often, both academia and private researchers concluded that by transferring a portion of cyber risk to an insurer, the insured could be psycho-economically inclined to keep the premium to a minimum. As a result, the insured will be less interested in retaining cyber risk and more interested in mitigating it (Yurcik & Doss, 2002; Kesan et al., 2005). One of the critical dependencies in this schema was the insurers' ability to accurately quantify cyber risk and then use the outcome to appropriately price cyber insurance premiums. If an insurer can accurately quantify cyber risk into an attractive premium, it may translate into a profit cove. On the other hand, when the price is set too low or too high, insurers risk to either lose a share of the market or to incur significant losses (Majuca et al., 2006).

In the past fifteen years, there has been little academic participation or contribution to the topic of cyber insurance from the information security community. It is rather ironic, given the close partnerships between technology and insurance companies during the e-commerce era (Enos, 2000). Recently, there has been a renewed

interest from information security experts concerning several topics related to cyber insurance. SANS, in partnerships with Allianz and Advisen, reported on “conceptual gaps that often make it difficult for members of the cyber security and cyber insurance communities to find a common basis on which to develop reasonable standards of security and insurability” (Filkins, 2016). The consequent study addressed how to "resolve these gaps, making cyber insurance an integral and highly valued part of a comprehensive InfoSec program” (Filkins, 2016a).

Another topic of great interest is how insurance underwriters determine the risk profile of potential insureds and set the pricing for cyber insurance premiums (Toregas & Zahn, 2014; Clinton & Reddy, 2015). This paper draws from the body of research and studies in the areas of cyber insurance, regulatory compliance, data privacy laws, and information security frameworks. Using CIS Critical Security Controls for Effective Cyber Defense, henceforward CIS Critical Security Controls, and a set of its accompanying metrics (Measurement Companion) will be explored to determine and to quantify the cybersecurity posture of insured organizations.

2. The Advent and Evolution of the Cyber Insurance

For the past three years, Marsh & McLennan have reported a steady increase in new cyber insurance policies, with over 30 percent increase each year in the number of US-based clients purchasing standalone cyber insurance (Marsh & McLennan, 2015). According to the annual 2016 Beeterly Report, more than ten insurers reported between 25 and 100 percent revenue growth, and two new entrants reported their revenues increased over 100 percent. In line with reported revenues, insurance industry experts forecast prosperous outlooks for the cyber insurance industry. PwC estimated the annual gross written cyber premiums would triple to $7.5bn by the end of the decade, and Swiss Re estimated that by 2025 there would be cyber coverage incorporated into every retail, commercial, and industrial policy (2015). By that timeframe, the global cyber insurance market is estimated to be well worth $85bn, according to Lloyd’s of London (Hartwig & Wilkinson, 2015).

It is not the first time the cyber insurance market is appraised to sharply inclined revenues. Back in 2001, for instance, the Insurance Information Institute estimated e-

commerce insurance premiums would reach $2.5bn by 2005, yet it took an extra decade (2015). This delay was mainly attributed to insurers' lack of experience with cyber risk and lack of reinsurance (or backstop) mechanisms to bail insurers out in the case of a "cyber avalanche" event. These and some other impediments lead to much higher cyber insurance premiums that made it a less desirable choice (Bandyopadhaay et al., 2009; Clinton, 2005; Pal & Golubchik, 2011; Toregas & Zahn, 2014). The supply and demand for cyber insurance products work differently than for the classic insurance in the sense that the demand drives the market and not the supply. Plus, cyber insurance is a sellers' market, unlike more developed/traditional business lines (Insurance Journal, 2015a) because current demand for comprehensive cyber risk solutions exceeds the supply (Willis Towers Watson, 2015). In this case, it is no longer just about underwriters' preparedness to insure cyber risk, but the ability to offer competitive pricing for cyber insurance policies to companies across all cyber risk profiles. Therefore, if the latest projections are accurate, not only there has to be a growing demand for cyber insurance products, but also insurers have to resolve impediments holding up the market growth. The following Sections will further explore whether or not current cyber insurance market conditions differ from a those a decade and a half ago.

2.1. E-Commerce Insurance

2.1.1. Contributing Factors

The growth of the dot-com bubble at the end of 1990's contributed to a dramatic increase in the frequency of cyber incidents. In 1998, there were about four thousand incidents reported. The number exploded in 1999 with nearly ten thousand incidents, following by over twenty thousand in 2000, over fifty thousand incidents in 2002, to over one-hundred and fifty thousand incidents in 2003 (McWilliams, 2001; Costello, 2002; CISS/CC, 2005). With the frequency of cyber incidents on the sharp incline, so was the range, sophistication, and coordination of cyber attacks, especially politically- motivated cyber attacks. During a single week in 2001, for example, close to 1,200 U.S. sites, including those belonging to the White House and other government agencies, were either subjected to a Distributed Denial of Service (DDoS) attack or defaced with pro-Chinese images (Vatis, 2002). In the same year, there was a triad of sophisticated

computer worms (Code Red, Nimbda, and Klez) in the period of three months, causing over $2bn in damages and cleanup; SQL Slammer followed in 2003 (Lyman, 2002).

As the number of cyber incidents grew, so did insurance claims and litigations. Due to the absence of standalone cyber insurance policies, companies were filing claims against whichever other business interruption policies they usually had, such as Commercial General Liability (CGL) or Errors and Omissions (E&O). However, these traditional policies were only meant to protect against the liability of "property damage," defined as "physical injury to tangible property" or "loss of use of tangible property that is not physically injured" (Rossi, 2001). Both insurers and business policyholders were understandably confused as to how traditional policies applied to e-commerce and scrambled to understand whether or not the electronically recorded or stored information was considered a "tangible property," and whether or not stored information was subject to "physical loss or damage." Insurers were also concerned about the significantly higher cost of defending and indemnifying cyber claims as compared to traditional claims. The number of lawsuits involving e-commerce claims could get exponentially higher, complexity and vagueness of international law and multi-jurisdictional disputes could bring uncertainty of courts' decisions, and there could be a significant cost for participation of technical computer experts (Jerry & Mekel, 2001).

In 1998, at the peak of the e-commerce boom, a new type of the cyber liability insurance emerged offering a specialized coverage for e-commerce exposures. It was often referred to as e-commerce insurance, or hacker insurance, that evolved from a collaborative venture between insurance and technology companies, counting insurers did not have cyber security expertise. From the economic perspective, these synergetic partnerships between insurers and security experts were considered idyllic: (i) insurers began underwriting standalone cyber insurance policies to cover first party claims (e.g., damage from denial-of-service attacks) because traditional policies were not designed or written with such attacks in mind, (ii) technology companies could offer their clients core technical services backed by the first party coverage or a comprehensive risk management solution and, (iii) organizations had the most comprehensive security protection, backed by a warranty from a reputable insurer. Peter Tibbett, who at the time

was the president of the International Computer Security Association (ICSA), the first technology company to offer warranty for its $40,000 per annum TruSecure service, said:

> *"We believe that we reduce the risk dramatically... Good enough is never going to be perfect. But we have a motivation to improve our service. If we have to write a check when someone gets hacked, it gives us another emphasis" (Poletti, 1998).*

By 2001, over a dozen insurers joined the trend with their specially crafted policies. Partnerships included some of the biggest names in both insurance and tech sectors: Cigna/Cisco, Sedgwick/IBM, Marsh McLennan/AT&T, Lloyd's of London/Counterpane, among others (Majuca, Yurcik, & Kesan, 2006).

In the absence of data privacy laws and industry-specific cyber regulations, IT security experts had little influence on the top management to adequately and diligently invest into IT security. Insurers, on the other hand, held power to incentivize the investment into IT security by discounting the insurance policy premiums for companies meeting adequate security standards. Security consultancy Counterpane Internet Security, for example, was offering customers of its managed security monitoring service the savings of 20 percent to 40 percent on insurance against the risk of losing revenue or critical information through network security breaches (Sayer, 2000). In another example from early 2001, J.S. Wurzler Underwriters, one of the first cyber insurance brokers/underwriters to start offering e-commerce insurance, was offering 20% discount to organization who followed their defined security standards. At that time, an ongoing spree of Internet worms actively targeted and exploited vulnerabilities in the Internet Information Services (IIS), one of the Microsoft's flagship products. With each exploit, Microsoft had to scramble issuing security updates to resolve it. When John S. Wurzler voiced his concern about several design flaws in Windows NT and proposed a surcharge of 5 percent to 15 percent to e-commerce insurance premiums for organizations that vastly relied on Microsoft products, he inadvertently sparked a lot of controversy for a much-impassioned topic (Olivia, Bryce, 2001). Mr. Wurzler shortly received a call from Microsoft representatives and clarified the main reason for the increase was not due to vulnerabilities in Microsoft's products, but due to the turnover rate of system administrators at companies using Microsoft operating systems. Since the high turnover rate could often exceed 33% annually, it would increase the likelihood of a security

incident and justify the increase in insurance premiums. "It caused some consternation," Mr. Wurzler explained, "But, at the same time, it caused companies to understand the situation" (Ceniceros, 2001). This example demonstrates the influence cyber insurers had in the technology sector.

2.1.2. Impediments

The prospect of cyber insurance market seemed so promising, that Bruce Schneier, then CTO of Counterpane Internet Security and now a renowned security technologist, envisioned:

> *"Eventually, the insurance industry will subsume the computer security industry… This is sometimes hard for computer techies to understand, because the security industry has trained them to expect technology to solve their problems… The real world doesn't work this way. Businesses achieve security through insurance… Sooner or later, the insurance industry will sell everyone anti-hacking policies. It will be unthinkable not to have one" ("The Insurance Takeover," 2001).*

In practice, however, quantifying cyber risk turned into insurance conundrum with many obstacles hindering the adoption of cyber insurance. First, there was a lack of statistical data about cyber incidents leading to a very limited actuarial support that largely relies on statistical data. Understandably, organizations were not interested in disclosing such information, whether to hide their reckless behavior or out of their fear of publicity and the possibility of losing the market edge to competitors (Baribeau, 2015). A lack of statistical data about cyber incidents also made it hard to predict a trend of cyber threats because usually a trend develops based on occurring incidents (Allen, 2004). Second, there was the issue with information asymmetry often resulting in subsequent issues with (i) moral hazard, when organizations may be less diligent to invest into mitigating cyber risks, since it may be more cost effective just to buy cyber insurance and, (ii) adverse selection, when insurers cannot distinguish between different risk types of insureds (Kesan, Majuca, & Yurcik, 2005a). Third, there was the issue of the interdependent and correlated nature of cyber risk, when one incident might ignite a chain of other related and unpredictable incidents. Any one of such events may become catastrophic for insurers in terms of total losses (Kunreuther & Heal, 2003; Ogut et al., 2005; Bohme & Kataria, Mukhopadhyay et al., 2006).

The burst of dot-com bubble had a direct effect on partnerships between technology companies and insurers, which would soon diminish. Many technology companies were either bankrupt, acquired by other companies, or surviving with only a small percentage of their once unlimited capital. Without this partnership, insurers did not have the expertise or cost-effective means to correctly distinguish the risk profile of insureds based on their cyber security posture (Bandyopadhaay et al., 2009; Bohme & Schwartz, 2010; Pal, 2012). One of the original solutions to address above mentioned problems was for insureds to undergo *ex-ante* rigorous risk assessment of their cyber security posture that would allow insurers to charge policy premiums according to risk classifications. In practice, though, it became rather an exception than the norm that cyber insurers differentiated policy premiums based on the security practices of their insureds (Anderson et al., 2008). Combined, these impediments lead to much higher cyber insurance premiums that made it a less desirable choice (Bandyopadhaay et al., 2009; Clinton, 2005; Pal & Golubchik, 2011; Toregas & Zahn, 2014). Many analysts believed the resolution would be merely a matter of time, yet more recent papers acknowledged the market had failed to grow as expected (Bohme & Schwartz, 2010).

2.2. The Next Wave of Cyber Insurance

2.2.1. Contributing Factors

It is not a coincidence the next wave of the rising cyber insurance market is happening hand- in- hand with the infinitely growing number, sophistication, and intensity of cyber incidents (Advisen, Zurich, Ernst & Yong, Marsh and McLennan, PwC, Lloyd's of London, 2015). It should be no surprise as to why World Economic Forum elected cyber risk into the top ten global risks category (2015). Practically no industry, no sector has been spared from being adversely affected by cyber breaches (Verizon DBIR, 2012-2016). In the U.S. alone: Yahoo!, LinkedIn, Gmail, Dropbox, MySpace, Adobe, Ebay, American Express, Chase, Target, Home Depot, Sony, VWF, OPM, DNC, and many more, all recently reported massive cyber breaches. To Willis Towers Watson, a prominent global multinational risk management, insurance brokerage and advisory company, it’s not surprising that the number of businesses considering purchasing cyber insurance is increasing:

Microsoft Office User

> *"Growing technology risks associated with the expansion of the mobile workforce, broad adoption of 'bring your own device' (BYOD) policies, and innovations, such as wearable technologies and the Internet of things (IoT), will only expand threats to data privacy and security. Cyber-attacks and data breaches are likely to be the rule rather than the exception for businesses of all types going forward." (2016).*

In fact, the global insurance industry itself was no exclusion. A French mutual insurance company experienced an internal breach in 2012, leading to cases of identity theft and false insurance claims. In 2015, Anthem Blue Cross Blue Shield and Premera Blue Cross experienced data breaches, exposing the personal information of up to 91 million policyholders. The same year, two German insurance groups were threatened with DDoS if a ransom of forty bitcoins would not be paid. Those and similar breaches amplify and justify the need for protection against the first and third party claims, not commonly covered by traditional insurance policies due to exclusions of services related to cyber incidents, e.g., forensic investigations, legal counsel, or settlements and judgments (IAIS, 2016). As the numbers, sophistication, and intensity of cyber incidents keep rising exponentially, many organizations who did not consider getting a cyber insurance policy or did not find cyber insurance to be cost effective, are now reconsidering (Hartwig & Wilkinson, 2015; Advisen 2016).

Cybercrime, however, is not the only contributing factor to fuel the demand-side of the current cyber insurance market. The proliferation of data privacy laws and industry-specific cyber regulations forced many organizations to rethink the way they had been doing business. In 2002, the State of California Legislative Counsel signed into law the first- of- its- kind State Bill 1386 to enforce the privacy of California residents' personal information. By 2016, forty-seven states, plus the District of Columbia, Guam, Puerto Rico and the Virgin Islands, all have enacted legislations requiring private, governmental or educational entities to notify individuals of security breaches involving misappropriation of personally identifiable information. In addition to data privacy laws, there have been many emerging industry-specific cyber regulations, such as HIPAA HITECH Act, PCI DSS, SEC Cybersecurity Initiative, and CFTC/NFA Interpretive Notice. Nonetheless, over 5 billion records have been lost globally to cyber breaches since 2013, emphasizing the need for even stronger privacy laws (Breach Level Index,

2016). As a result, many states have already been engaged to make these laws even tougher by expanding: (i) the definition of "personal information," e.g., to include medical, insurance, or biometric data, (ii) the definition of constitutes a data breach, (iii) types of organization that must comply with cyber law in a given state and, (iv) data breach notification requirements, e.g., timing and methods of notice, and who must be notified (National Conference of State Legislatures, 2016). In Tennessee, for example, recently signed into law SB 2005 requires data breach notifications even if breached data was encrypted (2016). In New York, the newly proposed cyber law, 23-NYCRR-500, will require covered financial organizations to protect any of its publicly available electronic information, plus the annual penetrations tests and quarterly vulnerability assessments. Then, at the end of every calendar year, organizations must submit the "Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulation" (NYDFS, 2016).

The new regulations have considerably increased the awareness of cyber risk and, "with that in mind, cyber insurance is gaining more promotion and regulators are encouraging companies to buy it to help manage their risks and minimize the cost of a breach (Insurance Journal, 2015a). To navigate the plethora of changing requirements for local state, federal, and international laws and regulations, organizations look into cyber insurance policies that cover expenses of legal counsel, regulatory action defense that also covers fines and penalties, credit monitoring for victims of a data breach, crisis management and public relations, consequential damages, business interruption loss and data recovery, cyber extortion, and more.

2.2.2. Impediments

Cyber insurance has finally grown into a multi-billion-dollar market with lucrative projections, yet questions still arise whether the current situation is any different from a decade ago. It is prudent to understand whether insurers have been able to overcome problems with insuring cyber risk, or whether cyber insurance impediments, such as quantification of cyber risk and accurate pricing of cyber insurance premiums, can continue hindering the cyber insurance market revenue and adoption rate.

A large amount of statistical data about cyber breaches has been accumulating as a result of requirements imposed by data privacy laws and regulations. Even though more cyber incidents have been reported in recent years, much of historical data maybe obsolete for modeling cyber risk, due to the constantly evolving complexity and vectors of cyber attacks. The American Academy of Actuaries concluded that "these changes limit the usefulness of historical data for predicting future costs of cyber-risks" (2016). For example, in one of the trending "low-cost, high-reward" scams, called Business Email Compromise (BES), cyber criminals mainly use social engineering to study and accurately identify individuals and protocols necessary to perform wire transfers in victim's environment. Instead of complicated hacking or malware techniques, a trivial email phishing is often used to trick victims into executing unauthorized transfers of funds. Yet, according to FBI, combined losses for domestic and international BES victims in the past few years topped $3.1bn (2016). It demonstrates just how unpredictable cyber risk may be.

Information asymmetry was another problem to hinder the adoption of cyber insurance. To cope with related impediments, e.g., adverse selection and moral hazard, insurers enhanced the underwriting process with a more thorough screening of prospective insureds. A typical cyber insurance purchase first involves a consultation with an insurance agent or broker to understand the nature of the business and likelihood of overall exposure to cyber security losses. Following, prospective insureds fill out a questionnaire about their cyber security posture, including the level of their self-protection, i.e. investments made to reduce the probability of the loss. Underwriters then use this information to assess if a prospective insured would fit into the insurer's risk appetite and to evaluate prospective insured's risk profile for determining policy coverage limits and the cost (Gleason, 2016). This underwriting process, however, has been under much scrutiny in the past decade and deemed as static incapable to cope with the dynamic nature of cyber risk landscape that changes daily (Weatherford, 2016). There have been several issues with the process. To start, most non-administrative sections in cyber insurance questionnaires often consist of "yes/no" or similar checkbox-type questions meant to assist underwriters in assessing relative risks. More often than not, these questions can be described as too vague and outdated, let alone static "yes/no" or

checkbox answers. Common cliché questions inquire whether or not a prospective insured has an anti-virus, a network firewall, or an intrusion detection/prevention system. While these questions in its simplest form may have been sufficient in early days of the cyber insurance market, they cannot possibly reflect prospective insured's exposure to today's cybersecurity losses. Cyber risk has vastly evolved in the past decade, and so have multiple layers and tiers of security tools. For instance, there is a free version of anti-virus software that excludes real-time protection and other critical features, and then there is an enterprise-grade endpoint protection software that incorporates the latest features. Similarly, there are rudimentary network firewalls versus the ones packed with Universal Threat Management (UTM) features. By not being able to distinguish if the answer to the question conforms to an adequate level of self-protection, underwriters increase the chance of misclassifying insureds and accumulating "bad" risk.

Another problem with the cyber insurance underwriting process has to do with the first-party attestation, where prospective insureds provide answers to questions posed in cyber insurance questionnaires at their sole discretion and based on their self-assessment of cyber risk. When comparing a cyber insurance underwriting process to a similar one for life insurance, underwrites tend not to trust applicants with self-assessment of their health conditions and instead rely upon a third-party performing a medical health assessment. In the case of cyber insurance, underwriters rely on prospective insureds' answers to determine a cyber risk profile, in spite of it being rather trivial for a prospective insured to provide inaccurate answers, whether deliberately or inadvertently. To protect themselves against fraudulent information, cyber insurers have been stipulating in the policy contracts they will not be liable for losses or claims arising from the insured's failure to maintain the same or higher level of security than the one in place at the policy inception (Kesan, Majuca, & Yurcik, 2005a). Nonetheless, according to the 11th Annual Global Information Security Survey conducted by PwC in partnership with CSO Magazine, the chances could be higher for misinformed answers than deliberately incorrect ones. The survey showed that out of over 9600 executive level participants, 84 percent of CEO's and 82 percent of CIO's believed their information security programs were effective in its current state. Even 78 percent of traditionally cautious CISO's shared the same level of confidence. Despite the way participants perceived information security

posture in their organizations, the actual number of successful security incidents was doubling every year (Hulme, 2013). Therefore, chances may be much higher for whoever is responsible for handling cyber insurance questionnaires to inadvertently exaggerate provided information. Instead of relying on the first-party attestation, cyber insurers could either involve a third-party to perform a risk assessment or do it on their own. In practice, however, there are additionally underlined problems discussed next.

Cyber insurance market growth presents a lucrative opportunity to both large insurance underwriters and new entrants. Beeterly Report found the latest state of cyber insurance market so profit-making, that "no insurers reported negative growth; in this market, if they had, it would have been shocking" (2016). This opportunity, however, comes at a great risk to new entrants due to lack of an insurance backstop similar to the Terrorism Risk Insurance Program Reauthorization Act (TRIPRA) – a federal backstop program for the private terrorism risk insurance market. Without a backstop to cover for significant losses caused by a catastrophic cyber incident, many insurers face the possibility of being wiped before they build up sufficient reserves to cover large losses. As Perkins explained:

> *"Underwriters are growing concerned about their exposure to one breach which affects many of their insureds simultaneously. Anthem's breach was the first that affected the market in this way and is being used as an example for underwriting management teams and regulators to inquire about systemic exposures involving multiple insureds" (2015).*

Therefore, the survival for new entrants depends on expanding their customer bases as rapidly as possible and accumulating as much revenue as possible. The presence of competitive cyber-insurers limits the possibility of slowing down the underwriting process and performing a comprehensive risk assessment. Even if one insurer is diligent enough to require a risk assessment, another insurer may write the policy without it. Insurers may end up with a portfolio of policies of unknown aggregate risks. In turn, it potentially leads to higher priced policies, accumulation of bad risk, and deterioration of incentives for good security practices (Shetty et al., 2010). In response to this trend, credit rating agencies warned insurers that the accumulation of cyber risk might negatively affect their ratings (A.M. Best, Moody's, Stadard & Poor's, 2015; Fitch Ratings, 2016).

A lack of the underwriters' cybersecurity expertise is another obstacle in improving the underwriting process. Underwriters have little insights into complexities of IT security and are often incapable to assess a security posture of potential insureds. According to Verisk Analytics, the leading provider of predictive analytics and information about risk, "the alignment of two sets of technical expertise, underwriting, and cybersecurity, are not easily found together. Insurance carriers that are not investing in specific cyber underwriting expertise are very often not able to drive to the market as strongly as those that do" (2016). In Hanover Research survey among cyber insurers, 82 and 53 percent of respondents admitted learning about cyber security news and information through the media and national news, respectively. Whereas, only 24 percent relied on the data from reputable sources, such as cyber security firms and blogs. When asked about what information they considered to be the most important for underwriting cyber risks, respondents predictably named the enterprise risk management philosophy and the nature of stored records or data as most important. Only 20 percent considered insured's due diligence with securely storing data, performing cyber security tests and audits, or employing network security and data encryption technologies (2014). A similar outcome could be observed in other reports, that for underwriters the risk acts as a tool for gauging the probability of events, rather than a direct measure of harm or loss (Filkins, 2016). Albeit, when Radichel dissected the anatomy of Target's data breach, one of the costliest data breaches with well over $300mn price tag, it revealed systematic deficiencies in technical security controls rather than in governance and risk management (2014). Target's data breach demonstrates how immensely important it should be for underwriters to enhance their overall expertise in cyber security. This necessity is explained: "It is only with that understanding that underwriters will be able to minimize risk, maximize profits, and provide insured organizations with the protection they need" (Lyon, 2016). Meanwhile, 51% admitted to having no dedicated cyber insurance underwriters and reliance on staff from other lines to sell cyber policies (Verisk Analytics, 2014).

Despite much effort to resolve aforementioned impediments, it is evident they contribute to unattractive pricing and remain hindering wider adoption of cyber insurance

(Pal & Golubchik, Herath & Herath, 2011; ENISA, 2012; Willis Towers Watson, 2015). A PwC report confirmed:

> *"Insurers and reinsurers are charging high prices for cyber insurance relative to other types of liability coverage to cushion some of the uncertainty. They are also seeking to put a ceiling on their potential losses through restrictive limits, exclusions, and conditions. However, many clients are starting to question the real value these policies offer, which may restrict market growth" (2015).*

For the cyber insurance market to grow as expected, cyber insurers must find better ways of assessing cyber risk and accurately calculating policy premiums. Refining the underwriting process that will enable insurers to efficiently write new policies while fully understanding the risk posture of insureds could be the start.

3. "Dynamic" Solutions for a "Static" Problem

3.1. Partnership between IT and Insurers

Back in 1998, insurers and IT security experts partnered to create a new type of insurance. Since then, Information Security has been one of the most sensitive topics discussed at any level of organizational management. It has evolved from the back of IT rooms and into its independent organizational structure on the government level (The White House, ENISA, 2016). It used to be that many businesses and IT managers claimed their understanding and adequate expertise in cybersecurity and necessary cybersecurity measures. According to the Barkly survey (2016), 70% of executives were confident about their current security solutions, even though only 50% of IT professionals shared this sentiment. Given never-ending data breaches, many organizations turned away from CEOs and other C-suite executives expanding into informational security roles and have invested into dedicated CISO/CSO's with emphasis on information security programs and risk management.

Recently, new partnerships began to reform between leaders in the cyber insurance and the information security parallels: AIG with RSA, IBM, K2, BitSight, AxioGlobal, and RiskAnalytics (AIG, 2016); Symantec with a re-insurer, Guy Carpenter. Nevertheless, a recent SANS study conducted in conjunction with Advisen shed light on gaps in a dissimilar understanding of cyber risk between insurance underwriters/agents, CEO's, and CISO's. These competing understandings included differences in

terminology, risk assessments, and frameworks, communications, or investment strategies. For example, participants of the survey representing cyber insurance industry were concerned that despite CISO's involvement in the insurance procurement process, they rarely understood the full value of cyber insurance or why they were not the decision makers. At the same time, the study showed how C-level could influence the perception of the role of cyber insurance in cyber programs and the decision whether to insure cyber risk.

One of the barriers cited in the survey was the absence of common cyber security standards, best practices, and metrics. A conclusion was made that in order "to evolve freely, the cyber security and insurance markets need a flexible standard that can serve as a directional indicator" (Filkins, 2016a). The standard also needs to include the most important items from the priority lists of both underwriters and security organizations:

> *"How can this framework achieve an insurable cyber posture and a higher level of security assurance? What metrics can evaluate the resulting risk profile to the underlying goals and objectives of the business? What services and tools can measure and continuously assess cybersecurity risk and the effectiveness of controls?" (Filkins, 2016b).*

3.2. Frameworks and standards

In 1998, in his speech, "Risk Management Is Where the Money Is", Dan Geer proposed the need to embed risk management into information security. Many information security frameworks have been developed since, whether by the private entities (e.g., COBIT 5 by ISACA, 27001/2:2013 by ISO, CIS Critical Security Controls), governmental entities (e.g., NIST in the U.S, ENISA in the European Union, ASD in Australia), or by industry-sponsored entities (e.g., Payment Card Industry Council). By gauging the cybersecurity preparedness against these frameworks, the insurers and risk managers can better understand gaps or adjust the strategy for achieving cyber maturity.

Albeit many similarities, these frameworks principally differ by their complexity, purpose, and the time and cost to adopt. COBIT 5, as an example, is a comprehensive and leading framework for aligning IT governance and objectives with enterprise's (ISACA, 2016). ISO 27002, on the contrary, provides a general, flexible layout for information management to help comply with laws and regulations, but does not provide a specific actionable path for achieving the required level of compliance. From the information

security perspective, these “grand” frameworks reflect the breadth and depth of organization’s cybersecurity posture, but from insurer's perspective, there are caveats regarding the time and cost. At the least, it would most certainly require third-party attestation, which may consume a significant percentage of the premium. In light of that, the majority of respondents in the Advisen Underwriter Survey agreed that the NIST and ISO 27000 frameworks were only “somewhat helpful” (Filkins, 2016a). It is worth noting, however, that some insurers require and facilitate security risk assessments for the insureds; a favorable assessment may help to lower the insured’s premium (Beeterly Risk Consultants, 2016).

Taking into consideration the above factors, Critical Security Controls should be considered an overall efficient method for cyber insurance underwriting processes. The following sections will address questions posed by Filkins (2016a) referring to a common security framework: how it can achieve an insurable cyber posture and a higher level of security assurance; how related metrics could be used to evaluate the resulting risk profile to the underlying goals and objectives of the business; and, how Critical Security Controls related services and tools would measure and continuously assess cybersecurity risk and the effectiveness of controls.

3.3. Why CIS Critical Security Controls?

One of the hindering impediments for the cyber insurance market has been a lack of statistical data about cyber incidents, as mentioned earlier in this paper. Ironically, actuaries were not the only ones. For quite some time, the IT security community itself could not prioritize their defense efforts because organizations did not want to report cyber incidents, or only reported incidents to law enforcement entities. In the US government sector, for instance, NSA held years of information about cyber incidents across government organizations. Moreover, since the 2000s the agency has been refining a list of mitigating security controls that would be most effective in stopping known attacks so that all government organization can better prioritize cyber security spending. The mandate from the US Department of Defense was that these mitigating controls would "first fix the known bad’s." It meant that no control should be made a priority unless it could be shown to stop or mitigate a known attack. Then, in 2008 NSA agreed to

collaborate with the security community, which started the development of CIS Critical Controls. One of the biggest differentiating factors of CIS Critical Security Controls from most others was the inheritance of the same principal that no control would be made a priority unless it mitigates a known attack. In 2009, the prioritized list of CIS Critical Security Controls was tested against eighty-five thousand computer systems across the U.S. State Department and achieved 88% reduction in vulnerability-based risk (SANS, n.d.). Since then, these controls have been regularly refined by a consortium of most prominent security experts from international, public, private, and governmental entities, so that only actual attack information could be used to justify adding new controls.

3.4. CIS Critical Security Controls: a tool for cyber insurance underwriters

Cyber insurance underwriters have predominantly relied on questionnaires with static checkboxes that focus on insufficient threat vectors and risk controls. This traditional methodology has been proven fundamentally flawed and insufficient for accurately determining the effectiveness of implemented security controls, prospective insureds' risk profiles, and setting premiums for cyber policies. CIS Critical Security Controls, on the other hand, along with developed assessment tools and measurement guides, can serve as a core methodology for both pre- and post- binding phases of the underwriting process.

There are distinct advantages of using CIS Critical Security Controls, as compared to other emerging methodologies. One of the biggest advantages is that CIS Critical Security Controls have become one of the de facto standards for "reasonable security" and have been recommended for adoption by many state, federal, and international cyber laws and regulations. Importantly, these are the same cyber laws and regulations that fuel the demand for cyber insurance products. In 2016, for example, California's Attorney General, Kamala D. Harris, determined that CIS Critical Security Controls "define a minimum level of information security that all organizations that collect or maintain personal information should meet," noting that "the failure to implement the controls that apply to an organization's environment constitutes a lack of reasonable security" (California Data Breach Report). There are other states which have already adopted a statue for "reasonable security measures," including Florida, Utah,

Maryland, Arkansas, Nevada, among others (National Conference of State Legislatures, 2016). By gauging insureds' actual practices against CIS Critical Security Controls, not only underwriters can assess the state of prospective insured's cybersecurity posture, but also the state of compliance with cyber laws and regulations. Should there be a data breach or another cyber-related incident, chances are a prospective insured will be a subject to regulatory penalties, among all other financial costs entailed by an incident, which will be later claimed against the cyber policy. Therefore, underwriters will also be able to better assess the probability of the loss.

Another advantage of integrating CIS Critical Security Controls into the underwriting process is about promoting holistic self-protection using cybersecurity best practices. CIS has specifically developed an ecosystem of free tools and documentation to aid anyone, whether a security expert or not, with the prioritized implementation of critical security controls, measuring the progress with ready-to-use metrics, conducting self-assessments and self-audits (Center for Internet Security Toolkit, 2017). Furthermore, underwriters can use this approach to standardize on using this comprehensive toolkit for establishing and customizing a streamlined process to determine insureds' cyber risk exposure during the pre-binding phase, as well as validating continuous improvement to insureds' cybersecurity posture and culture against evolving threats on the long-term.

Cyber Hygiene toolkits, along with A Measurement Companion to the CIS Critical Security Controls, provide recommended measures (i.e. recommended questionnaire questions) and metrics (i.e. recommended thresholds) for each one of twenty controls to help determine cyber risk exposure and to provide indications as to which risks may not have been identified. Cyber insurance underwriters can cost- and time- efficiently refine their questionnaires according to insurer's risk appetite or prospective insured's industry and cyber risk exposure. According to the Center for Internet Security, "the Cyber Hygiene Campaign is a multi-year effort that provides key recommendations for a low-cost program that any organization can adopt to achieve immediate and effective defenses against cyber attacks" (2014). Cyber Hygiene incorporates: (i) the methodology to prioritize efforts and investments into cyber security - Count, Configure, Control, Patch, and Repeat, (ii) toolkits that provide the information

and instructions for organizations to improve their cybersecurity posture and, (iii) a unique Executive Measurement Guide to assist the management with in the implementation of toolkits. The Cyber Hygiene Priority cycle is:

1. *Count* and periodically update an inventory of all computer systems and installed software on your network.
2. *Configure* key security settings and ensure these settings are deployed across all systems and networks in your organization's inventory.
3. *Control* as to who in your organization has administrative privileges to change, bypass, or override security settings. Revoke all default administrative privileges and institute a process to only grant it on a "need to have" basis.
4. *Patch* all computer systems, network devices, and software in your organization on a set periodic schedule.
5. *Repeat* this "cycle of events" to re-assessing for new cyber risks that can potentially affect your organization.

Cyber Hygiene is developed to be dynamic and to continue staying on par with changing cyber threat landscape. Each of the aforementioned recommendations in the Cyber Hygiene Priority cycle comes with a dedicated toolkit with easily understood instructions to improve organizations' cybersecurity posture. For example, the Toolkit for Configure includes a Plain English Guide," a Technical How-To Guide," a "How to Measure Guide," "Additional Resources," and "Mapping to NIST Cybersecurity Framework" (CIS, 2015). Indeed, these controls may not immediately appear on the "top five security controls to implement" list of many security experts, let alone those with lesser security expertise. Possibly because there are no big buzz words in these controls, such as "Firewall," "Intrusion Prevention System (IPS)," or "encryption." Nonetheless, by working in concert with the rest of CIS Critical Security Controls, these are proven to reduce over 80 percent of cyber threats (CIS, n.d.). The concept of Cyber Hygiene can be compared to personal hygiene: take proper care of your health on a daily basis, and you will be less likely to face a health crisis down the road (Null, 2015).

Microsoft Office User

In line with the Cyber Hygiene Priority, some of the first questions to prospective insureds should be:

1. *Has the company created and continue to maintain a master database/log of all hardware and software found on company networks/devices?*
2. *Has the company deployed an automated asset inventory discovery tool to build an asset inventory of systems connected to an organization's public and private network(s)? E.g., active tools that scan through network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.*
3. *Has the company identify and documented the number of outbound paths to the Internet and ensured that all paths are authorized and transit through approved security devices (i.e., firewall, web filter, IDS, IPS)?*
4. *Has the company developed and implemented controls that both (1) prevent the use of unauthorized hardware and software and, (2) quickly identify and remove unauthorized hardware and software, if found?*
5. *How often does the company's hardware inventory/asset database get updated?*
6. *How long does it take to detect new devices added to the company's network (time in minutes)?*
7. *How long does it take to detect new software installed on company's systems (time in minutes)?*
8. *How long does it take to alert the company's administrators that an unauthorized device or software is on the network (time in minutes)?*
9. *How long does it take to isolate/remove unauthorized devices from the company's network (time in minutes)?*
10. *Are administrators or scanners able to identify the location, department, and other critical details about the unauthorized system, if detected?*

Underwriters can use these questions to determine deficiencies in the insureds' cybersecurity posture accurately. In turn, any organization can use it to prioritize their efforts of adopting security best practices.

Additionally, each question comes with its respective metric consisting of three "Risk Threshold" values. These values represent an opinion from experienced security

experts and are not derived from any specific empirical data set or analytic model (CIS, 2015). Nonetheless, underwriters may choose to use these values as a baseline and adjust it in respect to insurer's risk appetite or insureds' risk profiles. Using the question #9 above as an example, the time it would take to isolate/remove unauthorized devices from the company's network, recommended risk thresholds are: Lower risk (< 60 minutes), Moderate risk (< 1 day), Higher risk (1-7 days). This provides underwriters with an objective method for measuring the cyber risk of insureds and the of entire portfolio. Underwriters can use these baseline values to further develop their own scoring methodology, similar to the way FICO® score is used to help lenders predict consumer behavior and the likelihood of paying their bills on time (CFPB, n.d.). A score-based cyber insurance metrics can be used to help insurers identify prospective insureds who are more likely to file a claim. For instance, a cyber-diligent organization with lower risk baseline for the Cyber Hygiene may earn an equivalent score between 500 and 650. Higher scores can be awarded for the adoption of other critical security controls, periodic risk assessments, penetration tests, the number of years without an incident, etc.

4. Conclusion

The cyber insurance market is booming with lucrative projections, but not for the first time. This time, though, it is not just the two-dimensional partnership between insurers and technology, but the whole socio-technical system at full play where all players must work together to succeed. Insurers must solve the conundrum of appropriately pricing the ever-changing cyber risk, and it may require them to look beyond the past as being a common predictor of the future. Raising premiums or playing with deductibles and coverage limits as a knee jerk reaction to dynamic nature of cyber risk will not work. While the industry anticipates high premium growth by 2020, the cyber insurance underwriting process must improve to sustain any claims. By understanding, adopting, and using proven CIS Critical Security Controls, cyber-savvy underwriters will be able to determine whether or not given measures have been taken to reduce the potential for a significant claim and provide cyber-hygienic organizations with the protection and coverage they need.

Microsoft Office User

5. References

A.M. Best. (2015). *A.M. Best's View on Cyber-Security Issues and Insurance Companies.* A.M. Best Company.

Advisen Ltd, ZURICH. (2015). *Information Security And Cyber Liability Risk Management.*

AIG. (2016). *Cyber Insurance*. Retrieved from AIG: http://www.aig.com/business/insurance/cyber-insurance

Aite Group. (2016). *Cyber Insurance and Cybersecurity: The Convergence.* Aite Group, LLC.

Allen, G. (2004). *Cyber Risk and Insurance - A Reality Check.* Willis.

American Academy of Actuaries. (2016, December). *ESSENTIAL ELEMENTS: Managing the Risks in Cyberspace.* Retrieved from American Academy of Actuaries: http://www.actuary.org/files/imce/EE.CyberRisks.pdf

Anderson, R. J., Bohme, R., Clayton, R., & Moore, T. W. (2008). *Security Economics and the Internal Market.* Study commissioned by ENISA.

Baer, W. S. (2001). *Rewarding IT Security in the Marketplace.* RAND.

Bandyopadhaay, R., Mookerjee, V. S., & Rao, R. C. (2009, November). Why IT Managers Don't Go For Cyber-Insurance Products. *Communications of the ACM*, pp. 68-73.

Baribeau, A. G. (2015, July-August). Cyber insurance: the Actuarial Conundrum. *Actuarial Review*, pp. 31-38.

Barker, B. (2016, June 6). *Underwriting Cyber Insurance: The 3 Ps of Cyber Risk*. Retrieved from Cybernance: http://www.cybernance.com/underwriting-cyber-insurance-3-ps-cyber-risk/

Barkly. (2016). *2016 Cybersecurity Confidence Report.* Barkly.

Beeterly Risk Consultants. (2016). *The Beeterly Report: Cyber/Privacy Insurance Market Survey.* Beeterly Risk Consultants.

Betterly Risk Consultants. (2008). *Cyberrisk Market Survey.* Betterly Risk Consultants.

Biener, C., Eling, M., & Wirfs, J. (2015). *INSURABILITY OF CYBER RISK: AN EMPIRICAL ANALYSIS.* Institute of Insurance Economics.

BitSight. (n.d.). *BITSIGHT SECURITY RATINGS FOR CYBER INSURANCE*. Retrieved from BitSight: https://info.bitsighttech.com/datasheet-cyber-insurance-security-ratings

BLI. (2016, October 15). *Data Records Lost or Stolen since 2013*. Retrieved from Breach Level Index: http://breachlevelindex.com/

Blosfield, E. (2016, September 16). *New York Proposes 'Flexible' Cybersecurity Regulation for Insurers, Banks*. Retrieved from Insurance Journal: http://www.insurancejournal.com/news/east/2016/09/15/426583.htm

Bohme, R., & Kataria, G. (2006). Models and measures for correlation in cyber-insurance. *WIES.*

Bohme, R., & Schwartz, G. (2010). Modeling Cyber-Insurance: Towards A Unifying Framework. *Workshop on the Economics of Information Security (WEIS).* Harvard.

Bolot, J., & Lelarge, M. (2008). Cyber Insurance as an Incentive for Internet Security. *WEIS.*

Microsoft Office User

Bolton, A. M. (2004). *Synopsis of the Cybercrime Act 2001.* SANS.

Bryce, R. (2001, March 5). *Insurers Offer Incentives To Buy Hacker Insurance*. Retrieved from SecList.org: http://seclists.org/isn/2001/Mar/30

Bryce, R. (2001, May 29). *Windows raises hacking insurance prices*. Retrieved from ZDNet.com: http://www.zdnet.com/article/windows-raises-hacking-insurance-prices/

Caglar, A. (2015, January). *A new approach to risk assessment for cyber insurance*. Retrieved from Financier Worldwide: https://www.financierworldwide.com/a-new-approach-to-risk-assessment-for-cyber-insurance

Ceniceros, r. (2001, June 17). *Underwriter weighs IT staff turnover in pricing*. Retrieved from Business Insurance: http://www.businessinsurance.com/article/20010617/ISSUE01/10004270/underwriter-weighs-it-staff-turnover-in-pricing

Chess, D. M., & White, S. R. (2000). *An Undetectable Computer Virus.* New York: IBM Thomas J. Watson Research Center.

CIS. (n.d.). *Welcome to the CIS Controls*. Retrieved from Center for Internet Security (CIS): https://www.cisecurity.org/critical-controls.cfm

Clinton, L. (2005). *Cyber-Insurance Metrics and Impact on Cyber-Security.* Retrieved from The White house: https://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf

Clinton, L., & Reddy, D. (2015). Can Cyber Insurance Be Linked to Assurance? *RSA Conference 2015.* San-Francisco.

Cohen, F. (1987). Computer Viruses - Theory and Experiments. *Computers & Security*, pp. 22-35.

Connelly, J. (2016, March 14). *How to Sell Cyber Insurance in a Competitive Market*. Retrieved from IA Magazine: http://www.iamagazine.com/markets/read/2016/03/14/how-to-sell-cyber-insurance-in-a-competitive-market

Content, J. (2016, April 4). *Cyber insurance process becoming more rigorous for certain industry sectors, cyber risk conference hears*. Retrieved from Canadian Underwriter: http://www.canadianunderwriter.ca/insurance/cyber-insurance-process-becoming-rigorous-certain-industry-sectors-cyber-risk-conference-hears-1004088331/

Costello, S. (2002, July 18). *Security incidents up sharply in 2002*. Retrieved from IT World Canada: http://www.itworldcanada.com/article/security-incidents-up-sharply-in-2002/26009

Council of Europe. (2001, November 23). *Convention on Cybercrime: Details of Treaty No.185*. Retrieved from Council of Europe: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Covington. (2016, June 14). *Recent Cases Highlight Potential Pitfalls of New Cyber Insurance Products.* Retrieved from Covington: https://www.cov.com/-/media/files/corporate/publications/2016/06/recent_cases_highlight_potential_pitfalls_of_new_cyber_insurance_products.pdf

Coyne, C. J., & Leeson, P. T. (2005). *Who's to Protect Cyberspace.* George Mason University.

Microsoft Office User

Dalpiaz, F., Paja, E., & Giorgini, P. (2016). *Security Requirements Engineering: Designing Secure Socio-Technical Systems.* MIT Press.

Das, S., Mukhopadhyay, A., & Anand, M. (2012). Stock market response to information security breach: A study using firm and attack characteristics. *Journal of Information Privacy and Security*, 27-55.

Deloitte. (2016). *Insurers on the brink: Disrupt or be disrupted.* Deloitte Center for financial Services.

Digital Millennium Copyright Act, Public Law 105-304, 112 Stat. 2860 (105th Congress October 28, 1998).

Dittrich, D. A. (2002, June 12). *Developing an Effective Incident Cost Analysis Mechanism*. Retrieved from Symantec: https://www.symantec.com/connect/articles/developing-effective-incident-cost-analysis-mechanism

Dougherty, S. (2014, November 24). *Learning from Cyber History*. Retrieved from Verisk Analytics: http://www.verisk.com/blog/cyber/learning-from-cyber-history/

Drouin, D. (2004). *Cyber Risk insurance: A Discourse or preparatory Guide.* SANS.

Dupont, B. (2012). *The Cyber Security Environment to 2022: Trends, Drivers, and Implications.*

Earnst & Yong. (2015). *Make sure your company has adequate coverage.* Earnst & Yong.

Earnst & Young. (2015). *Global Insurance Outlook.* E&Y.

Edwards, C. (2001, July 10). *Insurance Offered Against Hack Attacks*. Retrieved from ABC News: http://abcnews.go.com/Technology/story?id=99343&page=1

Eisenberg, T., Gries, D., Hartmanis, J., Holcomb, D., M. Lynn, S., & Santoro, T. (1989, June). The Cornell Commission: On Morris and the Worm. *Communications of the ACM*, pp. 706-707.

Eling, M., & Schnell, W. (2016). *Ten Key Questions on Cyber Risk and Cyber Risk Insurance.* The Geneva Association.

ENISA. (2016, July 28). *The Directive on security of network and information systems (NIS Directive)*. Retrieved from European Commission: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

Enos, L. (2000, July 10). *Lloyd's of London To Offer Hacker Insurance*. Retrieved from E-Commerce Times: http://www.ecommercetimes.com/story/3730.html

eWeek. (2001, March 5). *You're Covered*. Retrieved from eWeek: http://www.eweek.com/c/a/Security/Youre-Covered

FBI. (2016, June 14). *Business E-mail Compromise: The 3.1 Billion Dollar Scam*. Retrieved from FBI Internet Crime Complaint Center (IC3): https://www.ic3.gov/media/2016/160614.aspx

FICO. (2016, October 27). *FICO Enterprise Security Score Gives Long-Term View of Cyber Risk Exposure*. Retrieved from FICO: http://www.fico.com/en/newsroom/fico-enterprise-security-score-gives-long-term-view-of-cyber-risk-exposure-10-27-2016

Filkins, B. (2016). *Bridging the Insurance/InfoSec Gap: The SANS 2016 Cyber Insurance Survey.* SANS & Advisen.

Microsoft Office User

Fitch Ratings. (2016, March 21). *Fitch: Rapid Growth in Cyber Insurance Would Be Credit-Negative*. Retrieved from Fitch Ratings: https://www.fitchratings.com/site/pr/1001233

Geddes Baribeau, A. (2015, July/August). Cyber Insurance: The Actuarial Conundrum. *Actuarial review*, pp. 30-38.

Geer, D. (1998, October 12). Risk Management is where the money is. *Digital Commerce Society of Boston.* Risks-Forum Digest. Retrieved from UC San Diego: http://cseweb.ucsd.edu/~goguen/courses/275f00/geer.html

Gleason, A. (2016, September 9). Retrieved from NIST: https://www.nist.gov/sites/default/files/documents/2016/09/15/aia_rfi_response.pdf

Gramm–Leach–Bliley Act, also known as the Financial Services Modernization Act of 1999, Pub.L. 106–102, 113 Stat. 1338 (106th United States Congress November 12, 1999).

Guy Carpenter. (2016, May 17). *Guy Carpenter Forms Strategic Alliance to Develop Cyber Aggregation Model.* Retrieved from Guy Carpenter: http://www.guycarp.com/content/dam/guycarp/en/documents/PressRelease/2016/Guy%20Carpenter%20Forms%20Strategic%20Alliance%20to%20Develop%20Cyber%20Aggregation%20Model%20May%2017%202016.pdf

Hanover Research. (2014). *Cuber Insurance survey.* Hanover Research.

Hartwig, R., & Wilkinson, C. (2015). *Cyber Risk: Threat and opportunity.* New York: Insurance Information Institute.

Herath, H. S., & Herath, T. C. (2011). Copula-based actuarial model for pricing cyber-insurance policies. *Insurance Markets and Companies: Analyses and Actuarial Computations*.

Hillman, K. R., & Hite, C. J. (2016, May). Has the fortress been hacked by consumers? Cyber class actions are gaining steam. *ACC Docket (Association of Corporate Counsel)*, 62-69.

Hoffman, M. A. (2016, May 29). *Prospect of catastrophic cyber attack triggers interest in insurance backstop*. Retrieved from Business Insurance: http://www.businessinsurance.com/article/20160529/NEWS06/306059995

IAIS. (2016). *Issues Paper on Cyber Risk to the Insurance Sector.*

Innerhofer–Oberperfler, F., & Breu, R. (2009). *Potential Rating Indicators for Cyberinsurance: An Exploratory Qualitative Study.* Innsbruck, Austria: University of Innsbruck,

Insurance Information Institute. (2015, October 21). *U.S. Cyber Insurance Market Demonstrates Growth, Innovation in Wake of High Profile Data Breaches*. Retrieved from Insurance Information Institute: http://www.iii.org/press-release/us-cyber-insurance-market-demonstrates-growth-innovation-in-wake-of-high-profile-data-breaches-102015

Insurance Institute of Canada. (2015). *Cyber Risks: Implications for the Insurance Industry in Canada.* Insurance Institute of Canada.

Insurance Journal. (2015, June 12). *Where Cyber Insurance Underwriting Stands Today*. Retrieved from Insurance Journal: http://www.insurancejournal.com/news/national/2015/06/12/371591.htm

Insure.com. (2016, August 9). *8 ways people blow their life insurance medical exams*. Retrieved from Insure.com: http://www.insure.com/life-insurance/how-people-blow-their-life-insurance-medical-exams.html

ISA/ANSI. (2010). *The financial management of cyber risk.* ANSI.

ISACA. (2016). *What is COBIT 5?* Retrieved from ISACA: http://www.isaca.org/cobit/pages/default.aspx?utm_source=2012-cobit5-brochure&utm_medium=direct-mail&utm_content=friendly-cobit5overview&utm_campaign=cobit5

Jerry, R. H., & Mekel, M. L. (2001). *Cybercoverage for Cyber-Risks_ An Overview of Insurers Responses to the Perils of e-Commerce.* University of Florida Levin College of Law.

Jones, M. (2014, November 5). *Increasingly Tough Market for Brokers*. Retrieved from Risk & Insurance: http://www.riskandinsurance.com/increasingly-tough-market-brokers/

Kark, K., Francois, M., & Aguas, T. (2016, July 25). *The new CISO: Leading the strategic security organization*. Retrieved from Deloitte University Press: https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/ciso-next-generation-strategic-security-organization.html

Kesan, J. P., Majuca, R. P., & Yurcik, W. (2005). *The Economic Case for Cyber-Insurance: In Securing Privacy in the Internet Age.* Stanford University Press.

Kesan, J. P., Majuca, R. P., & Yurcik, W. J. (2005a). Cyberinsurance As A Market-Based Solution To The Problem Of Cybersecurity—A Case Study. *Workshop on the Economics of Information Security.* Harvard, MA.

Ketron. (2016). *Senate Bill 2005.* Retrieved from Tennessee General Assembly: http://www.capitol.tn.gov/Bills/109/Bill/SB2005.pdf

Khan, R. (2010). *Practical Approaches to Organizational Information Security Management.* SANS.

Kitten, T. (2015, August 10). *Is Neiman Marcus Case a Game-Changer?* Retrieved from Bank Info Security: http://www.bankinfosecurity.com/neiman-marcus-suit-game-changer-a-8462

KPMG. (2016). *Cyber Insurance: Are insurers finding growth or looking for trouble?* KPMG.

Krebs, B. (2016, October 21). *Hacked Cameras, DVRs Powered Today's Massive Internet Outage*. Retrieved from Krebs On Security: https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

Kunreuther, H., & Heal, G. (2003). Interdependent security. *Journal of Risk and Uncertainty*, 26(2-3):231–49.

Kuypers, M. A., Maillart, T., & Paté, E. (n.d.). *An Empirical Analysis of Cyber Security Incidents at a Large Organization.*

Lai, c., Medvinsky, G., & Neuman, B. C. (1994). Endorsements, Licensing, and Insurance for Distributed System Services. *The Second ACM Conference on Computer and Communications Security.* Association for Computing Machinery.

Leagle. (2015). *ZURICH AM. INS. CO. v. SONY CORP. OF AM.* Retrieved from Leagle: http://www.leagle.com/decision/In%20NYCO%2020150501633/ZURICH%20AM.%20INS.%20CO.%20v.%20SONY%20CORP.%20OF%20AM.

Microsoft Office User

Lloyd's. (2015, May 28). *Vision 2025 and AAMGA*. Retrieved from Lloyd's: https://www.lloyds.com/news-and-insight/press-centre/speeches/2015/05/vision-2025-and-aamga

Lyman, J. (2002, February 21). *In Search of the World's Costliest Virus*. Retrieved from E-Commerce Times: www.ecommercetimes.com/perl/story/16407.html

Lyon, J. (2016). Minimizing Risks & Avoiding Lawsuits with Actionable Cyber Data. *Professional Liability Underwriting Society (PLUS) Journal*, 6, 13.

Majuca, R. P., Yurcik, W., & Kesan, J. P. (2006). *The Evolution of Cyberinsurance.* National Center for Supercomputing Applications (NCSA).

March & McLennan. (2016). *MMC Cyber Handbook 2016.* March & McLennan Companies.

Marsh & McLennan. (2014). *US Senate Passes Bill That Would Extend Federal Insurance Backstop*. Retrieved from Marsh & McLennan Companies (MMC): https://www.marsh.com/us/insights/research/us-senate-passes-bill-extend-federal-insurance-backstop.html

Marsh & McLennan. (2015). *Benchmarking Trends: As cyber concerns broaden, insurance purchases rise.* MARSH & McLENNAN COMPANIES.

Martin, S. (2016, June). *The cyberinsurance market is maturing rapidly, but there are still gray areas to navigate*. Retrieved from TechTarget SearchSecurity: http://searchsecurity.techtarget.com/feature/Cyberinsurance-policies-Getting-coverage-and-avoiding-limitations

McWilliams, B. (2001, October 15). *CERT: Cyber Attacks Set To Double In 2001*. Retrieved from Security Focus Newsbytes: http://www.securityfocus.com/news/266

Moody's. (2015, November 15). *Moody's: Threat of cyber risk is of growing importance to credit analysis*. Retrieved from Moody's: https://www.moodys.com/research/Moodys-Threat-of-cyber-risk-is-of-growing-importance-to--PR_339656

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2006). e-Risk management with insurance: A framework using copula aided Bayesian belief. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, (pp. 126a-126a).

National Conference of State Legislatures. (2016, January 4). *Security Breach Notification Laws*. Retrieved from NCSL: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

NYDFS. (2016, December). *New York State Department of Financial Services Proposed 23 NYCRR 500.* Retrieved from New York State Department of Financial Services: http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf

Ogut, H., Menon, N., & Raghunathan, S. (2005). Cyber insurance and IT security investment: Impact of interdependent risk. *WEIS.*

Olivia, V. (2001, June 8). *Premiums on Hacker Insurance Make Windows NT More Expensive*. Retrieved from Gartner: https://www.gartner.com/doc/331136/premiums-hacker-insurance-make-windows

Pal, R. (2012). *Cyber-Insurance in Internet Security: A Dig into the Information Asymmetry Problem.* University of Southern California.

Microsoft Office User

Pal, R., & Golubchik, L. (2011). *Pricing and Investments in Internet Security: A Cyber-Insurance Perspective.* IEEE.

Pal, R., Golubchik, L., & Psounis, K. (n.d.). *Aegis: A Novel Cyber-Insurance Model.* University of Southern California, USA.

Perkins, M. (2015). *Inside the Mind of Cyber Underwriter.* Lockton Companies.

PLUS. (2015). How to Sell Cyber Insurance to Different industries. *Cyber Liability Symposium.* Chicago, IL: Professional Liability Underwriting Society (PLUS).

Poletti, T. (1998, June 4). *First-Ever Insurance Against Hackers.* Retrieved from CNN.com.

Ponemon Institute. (2013). *Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age.* Ponemon Institute LLC.

PwC. (2015). *Insurance 2020 & Beyond: Reaping the dividends of cyber resilience.* PwC.

Radichel, T. (2014). *Case Study: Critical Controls that Could Have Prevented Target Breach.* SANS.

Rossi, M. (2000, May). *Bringing Order to Chaos: Insurance Issues for E-Commerce Activities*. Retrieved from IRMI: https://www.irmi.com/articles/expert-commentary/new-stand-alone-e-commerce-insurance-for-third-party-liability-claims-part-1

Rossi, M. (2001, August). *Is Computer Data "Tangible Property" or Subject to "Physical Loss or Damage"?* Retrieved from Insurance Risk Management Institute (IRMI): https://www.irmi.com/articles/expert-commentary/is-computer-data-tangible-property-or-subject-to-physical-loss-or-damage-part-1

Ryan, T. A., & Carbone, W. (2016, May 23). *Cyber liability insurance: As the market heats up, is it time to cool off in a pool?* Retrieved from Milliman: http://us.milliman.com/insight/2016/Cyber-liability-insurance-As-the-market-heats-up--is-it-time-to-cool-off-in-a-pool/#

S&P Global Market Intelligence. (2015, June 9). *U.S. Financial Services Credit Ratings Are Resilient To Cyber Security--For Now*. Retrieved from S&P Global Credit Portal: https://www.globalcreditportal.com/ratingsdirect/renderArticle.do?articleId=1403071&SctArtId=320688&from=CM&nsl_code=LIME&sourceObjectId=9203780&sourceRevId=4&fee_ind=N&exp_date=20250609-19:35:11

SANS & Allianz. (2016). *Quantifying Risk: Closing the Chasm Between Cybersecurity and Cyber Insurance.* SANS.

SANS. (n.d.). *CIS Critical Security Controls: A Brief History*. Retrieved from SANS: https://www.sans.org/critical-security-controls/history

Sayer, P. (2000, July 11). *Lloyd's of London Backs Insurance Against Hackers*. Retrieved from Computerworld: https://www.computerworld.co.nz/article/70044/lloyd_london_backs_insurance_against_hackers/

Schneier, B. (2001, February). *The Insurance Takeover*. Retrieved from Schneier on Security: https://www.schneier.com/essays/archives/2001/02/the_insurance_takeov.html

Schwartz, J. L., & Willmott, C. B. (2016). The State of Cyberinsurance Coverage Litigation: A Survey of Significant Decisions and Pending Litigation. *Professional Liability Underwriting Society (PLUS) Journal*, 1, 8.

Microsoft Office User

SecurityScorecard. (n.d.). *Security Benchmarking for Cyber Insurance*. Retrieved from SecurityScorecard: https://securityscorecard.com/solutions/cyber-insurance/

Shetty, N., Schwartz, G., Felegyhazi, M., & Walrand, J. (2010). Competitive Cyber-Insurance and Internet Security. In *Economics of Information Security and Privacy* (pp. 229-247). Springer US.

Simpson, A. (2016, April 12). *Federal Court Rules CGL Insurance Covers Data Breach*. Retrieved from Amazon Laws: http://www.insurancejournal.com/news/national/2016/04/12/404881.htm

Simpson, A. G. (2016, March 21). *Rating Agency Warns P/C Insurers on Taking On Too Much Cyber Risk*. Retrieved from Insurance Journal: http://www.insurancejournal.com/news/national/2016/03/21/402607.htm

Society of Actuaries. (2000). E-Commerce Series: Risk Management for the Internet. *San Diego Spring Meeting.* Society of Actuaries.

State of California Legislative Counsel. (2002). *SB-1386 Personal information: privacy. (2001-2002)*. Retrieved from California Legislative Information: http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=200120020SB1386

Statista. (2016). *Reasons for lack of suitable cyber insurance for companies in the United States 2016*. Retrieved from Statista: https://www.statista.com/statistics/422683/reasons-cyber-insurance-not-adequate-us-companies/

Stoll, C. (1989). *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.* Doubleday.

Swartz, J. (2003, February 9). *Firms' hacking-related insurance costs soar*. Retrieved from USA Today: http://usatoday30.usatoday.com/money/industries/technology/2003-02-09-hacker_x.htm

Target . (2015, February 25). *Target Reports Fourth Quarter and Full-Year 2014 Earnings*. Retrieved from Target: http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=2019880

The White House. (2016, July 26). *Presidential Policy Directive 41 - United States Cyber Incident Coordination*. Retrieved from The White House: https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

Toregas, C., & Zahn, N. (2014). *Insurance for Cyber Attacks: The Issue of Setting Premiums in Context.* Cybersecurity Policy and Research Institute.

USA Today. (2001, October 3). *Microsoft steps up software security*. Retrieved from USA Today: http://usatoday30.usatoday.com/life/cyber/tech/2001/10/3/microsoft-security.htm

Vatis, M. (2002). *Cyber Attacks: Protecting America's Security Against Digital Threats.* George Washington University.

Veerappa, B. (2015). *A Concise Guide to Various Australian Laws Related to Privacy and Cybersecurity Domains.* SANS.

Verisk Analytics. (2014, October 28). *Potential Growth in Cyber Insurance Linked to Customer Education in New ISO Survey*. Retrieved from Verisk Analytics:

Microsoft Office User

http://www.verisk.com/archived/2014/october/potential-growth-in-cyber-insurance-linked-to-customer-education-in-new-iso-survey.html

Weatherford, M. (2016). *Cybersecurity Insurance: The Catalyst We've Been Waiting For.* San Francisco: RSA Conference 2016.

Weber, A. M. (2003, January). The Council of Europe's Convention on Cybercrime. *Berkeley Technology Law Journal*, pp. 425-446.

WEF. (2015). *Global Risks 2015, 10th Edition.* WEF.

Willis Towers Watson. (2016). *State of the Cyber Market: Alert.* Willis Towers Watson.

World Energy Council in partnership with Marsh & McLennan Companies and Swiss Re Corporate Solutions. (2016). *The Road to Resilience: Managing Cyber Risk.* World Energy Council.

Yurcik, W., & Doss, D. (2002). *Cyberinsurance: A Market Solution To The Internet Security Market Failure.* WEIS.

Last Updated: July 26th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MDUS	Sep 25, 2017 - Sep 30, 2017	Live Event
Data Breach Summit & Training	Chicago, ILUS	Sep 25, 2017 - Oct 02, 2017	Live Event
SANS London September 2017	London, GB	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, DK	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, NL	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, COUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Oslo Autumn 2017	Oslo, NO	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS DFIR Prague 2017	Prague, CZ	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZUS	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, SG	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS AUD507 (GSNA) @ Canberra 2017	Canberra, AU	Oct 09, 2017 - Oct 14, 2017	Live Event
Secure DevOps Summit & Training	Denver, COUS	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VAUS	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, JP	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS Brussels Autumn 2017	Brussels, BE	Oct 16, 2017 - Oct 21, 2017	Live Event
SANS Berlin 2017	Berlin, DE	Oct 23, 2017 - Oct 28, 2017	Live Event
Security Awareness Summit & Training 2017	OnlineTNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced