~~Sponsored Captive Management in~~ Cyber Security Liability Insurance Addressed in a Sponsored Captive Insurance Company

A SeCAP Inc. White Paper
2023

1.0 Introduction

This white paper explores the concept of applying a Sponsored Captive Insurance model to address the complexities of insuring cyber security risk.

Traditional insurance models are failing cyber security insurance policy holders with the bottom-line result being extremely high premium costs and restricted policy coverage due to not having sufficient cyber security technical expertise~~high loss rates~~. As a ~~result~~result, insurance carriers are severely restricting policy language and increasing premium prices. Government supplied cyber security framework guidelines impart a need for insurance; thereby, increasing pressure on companies to carry policies with no clear benefit. The cyber security insurance industry ~~is in need of~~needs a new approach.

This paper establishes the benefit of a managed hybrid insurance/technical approach to cyber security insurance through a specific captive insurance structure called a "Sponsored Captive". This proposed structure allows for a sponsor to organize a legal regulatory approved captive insurance company complete with, legal, accounting and actuary functions~~for a captive insurance company~~ along with providing complimentary services relative to cyber security discovery and remediation. Policy holders will be able to use premium surpluses to invest in continual enhancement of security protection profile(s).

1.1 What Does Cyber Security Insurance Cover

Cyber Security Liability Insurance is a policy that covers a business in the event of a cyber attack or data breach. It can help offset the costs associated with recovery, including legal fees, data recovery data restoration, and public relations. Cyber Security Insurance works by providing financial compensation to a business in the event of a cyber attack. Once a policy is in place, the business owner pays a premium to the insurer. If a cyber attack occurs, the insurer will pay out compensation as specified in the policy.

1.2 What is a Captive Insurance Company

According to the Center for Insurance Policy and Research[1], a think tank of the National Association of Insurance Commissioners, the definition of captive insurance is, ***"… a captive is a wholly owned subsidiary created to provide insurance to its non-insurance parent company (or companies). Captives are essentially a form of self-insurance whereby the insurer is owned wholly by the*** **insured**[1]. Captive insurance companies have had a ~~long-standing~~long-standing history. The term "captive insurance" was first used in 1955 by Frederic Reiss, a property-protection engineer in Youngstown, Ohio. Reiss established the first captive insurance company in Bermuda in 1962. Since 1962 there has been significant growth in the number of captive insurance companies. As of 2022 there are over 7,000 captive companies globally[1]. By comparison in 1980 there were approximately 1,000[1]. Captive Insurance companies can be domiciled, or licensed, domestically in the United States or offshore. The number of captive domiciles is growing and remains competitive. With countless jurisdictions allowing some form of captive establishment[1]**.** Once established, a captive insurance company operates just like any other traditional insurance company[1].

1.3 What is a Sponsored Captive Insurance Company

Vermont has a robust captive insurance regulatory history. Through the Department of Financial Regulations in the Captive Insurance Division, Vermont has established, "***A captive insurance company represents an option of many corporations and groups that want to take financial control and manage risks by underwriting their own insurance rather than paying premiums to third party***

[1] Captive Insurance Companies (naic.org)
[2] Cyber Insurance Market Size, Trends | Overview Report [2030] (fortunebusinessinsights.com)
[3] Cybersecurity, liability, and your MSP - ThreatAdvice
[4] Companies are finding it harder to get cyber insurance (cnbc.com)
[5] Cybersecurity, liability, and your MSP - ThreatAdvice
[6] CSWP 29, The NIST Cybersecurity Framework 2.0 | CSRC
[7] Cyber Security Guidance Material | HHS.gov
[8] A Framework for Cybersecurity (fdic.gov)
[9] 33-11216-fact-sheet.pdf (sec.gov)
[10] https://www.cyberseek.org/
[11] Cybercrime | Europol (europa.eu)
[12] 15 shocking BYOD statistics from 2018 - 2023 (comparitech.com)

insurers"[29]. Vermont goes as far as to publish the benefits of captive insurance company establishment as:[29]:

The advantages of going captive are:

- ***Coverage tailored to meet your needs***
- ***Reduced operating costs***
- ***Improved cash flow***
- ***Increased coverage and capacity***
- ***Investment income to fund losses***
- ***Direct access to wholesale reinsurance markets***
- ***Funding and underwriting flexibility***
- ***Greater control over claims***
- ***Smaller deductibles for operating units***
- ***Additional negotiating leverage with underwriters***
- ***Incentives for loss control***
- ***Alternatives to the costly practice of trading dollars with underwriters in the working layers of risk***

2.0 Problem Setting:

2.1 Issues in Cyber Security

The need for digital transformation (hosted, public cloud, mobility and hybrid environments) across all market sectors combined with the complexity of threat actors and emergence of Artificial Intelligence (AI) has resulted in a threat landscape that has outpaced the insurance industry's ability to evaluate risk; thereby, negatively impacting resultant premiums and coverage[2]~~–~~.[2]. In a ~~nut shell~~nutshell, premiums are increasing and policy coverage is shrinking.

To counter emerging threats traditional insurance carriers have attempted to align with Managed Security Service Providers (MSSP's) to identify, protect, detect, respond and recover sensitive data before a catastrophic loss; however, these attempts have resulted in the unintended consequences of; 1) including the MSSP into the liability chain[3,5] ~~and;~~and 2) policy language restricting coverage for foreign born attacks[3].

Corporate executives may be subject to liability as National Institute of Standards and Technology (NIST) Framework 2.0 for year 2023 have recommended the inclusion of corporate governance standards in the event of cyber attacks[6]**.** NIST Cybersecurity Framework (NIST CSF) consists of standards, guidelines, and best practices that help organizations improve their management of cybersecurity risk. The NIST CSF is the derivative source for all other framework guidelines; such as Health Insurance Portability Accountability Act (HIPAA)[7]~~–~~,[7], Federal Deposit Insurance Corporation (FDIC)[8]**,** etc. The Securities and Exchange Commission (SEC) has announced its own regulatory requirement that breaches must be disclosed to impacted parties no later than ~~ninety-six~~ninety-six hours after any breaches have been discovered[9] or be subject to extensive fines.

2.2 The Incomplete Approach to Data Security

Data loss and theft has the potential to affect all of us – from private individuals to small businesses and multinational corporations. While awareness of the threat posed by a data breach is increasing, there is still a lack of understanding of the many ways in which such a breach can occur and, most importantly, little awareness of the often simple steps that can be taken to prevent personal and business data loss.

[1] Captive Insurance Companies (naic.org)
[2] Cyber Insurance Market Size, Trends | Overview Report [2030] (fortunebusinessinsights.com)
[3] Cybersecurity, liability, and your MSP - ThreatAdvice
[4] Companies are finding it harder to get cyber insurance (cnbc.com)
[5] Cybersecurity, liability, and your MSP - ThreatAdvice
[6] CSWP 29, The NIST Cybersecurity Framework 2.0 | CSRC
[7] Cyber Security Guidance Material | HHS.gov
[8] A Framework for Cybersecurity (fdic.gov)
[9] 33-11216-fact-sheet.pdf (sec.gov)
[10] https://www.cyberseek.org/
[11] Cybercrime | Europol (europa.eu)
[12] 15 shocking BYOD statistics from 2018 - 2023 (comparitech.com)

Many companies have taken at least some action to protect themselves through monitoring software, MSSP contracts, Information Tech (IT) training, etc. While this is important, breaches continue to expand in number and damage. Cyber security is not a one solution fits all proposition as internal networks, hardware, application stacks and cloud deployments compose part of compute surface area where attacks can be initiated.

Cyber security, as an industry, lacks enough qualified people creating a vacuum where cyber criminals are presented with almost no resistance. According to a 2022 industry poll CyberSeek (a nonprofit collaboration between CompTIA, NIST and Lightcast) discovered the following trends[10]:

- 3.5 Million Vacant Cybersecurity Jobs
- Average Breach Cost $3.8 Million
- 43% of SMB's have no Cyber Security Posture
- 52% of SMB's do not Have Access to Cyber Security Expertise
- 75% of Organizations Lack Breach Cybersecurity Plan
- 90,000 CISSPs & 106,000 Job Openings
- 17,000 CISMs & 40,000 Job Openings

This lack of qualification has a compounding effect as companies cannot find knowledgeable people to conduct the work of securing company assets against attacks.

2.3 The Ever Increasing Threat

The cost to businesses for data loss is increasing rapidly. European Union law enforcement agency Europol estimates loss associated with cybercrimes to reach eight trillion by end of 2023 and may reach as high as 10.5 trillion by 2025[11] Europol suggests the proliferation of attacks can be attributed to two main reasons. First is the automation of malware through artificial intelligence; whereby, bad actors no longer need to be able to write code to create and deploy an attack. Second, the complexity of botnets specific unknown store-and-forward capabilities.

Work from home policies embraced as a response to the COVID pandemic have dramatically increased the attack surface bad actors can exploit. Many companies deployed Bring Your Own Device (BYOD) policies where employee owned devices are used to access private company intranet(s) and sensitive data. The security guardrails tend to be less rigorous on personal devices. For ~~example;~~example, 96% of devices connected to corporate data assets are personal, only 51% of companies have a BYOD security policy in place, only 11% of employees are aware of corporate BYOD security policies[12].

.

[1] Captive Insurance Companies (naic.org)
[2] Cyber Insurance Market Size, Trends | Overview Report [2030] (fortunebusinessinsights.com)
[3] Cybersecurity, liability, and your MSP - ThreatAdvice
[4] Companies are finding it harder to get cyber insurance (cnbc.com)
[5] Cybersecurity, liability, and your MSP - ThreatAdvice
[6] CSWP 29, The NIST Cybersecurity Framework 2.0 | CSRC
[7] Cyber Security Guidance Material | HHS.gov
[8] A Framework for Cybersecurity (fdic.gov)
[9] 33-11216-fact-sheet.pdf (sec.gov)
[10] https://www.cyberseek.org/
[11] Cybercrime | Europol (europa.eu)
[12] 15 shocking BYOD statistics from 2018 - 2023 (comparitech.com)

2.4 Cyber Security Liability Insurance Coverage – The Weak Link in NIST Framework

Insurance companies reference the NIST Cyber Security Framework 2.0 ~~as a means to~~to shape cyber security profiles for "all sized entities"[13]**.** Traditional insurance carriers have relied on the NIST framework as a model to assess if a policy holder is protected. As the cyberspace has matured, the industry is in a whack-a-mole predicament where policies and coverage have been subject to constant change. Traditional insurance carriers have been trying to apply a standard risk profiling model where almost nothing is static.

3.0 Problem Setting – Insurance Industry

3.1 Traditional Insurance – A Failed Model

The scalability of cyberattacks presents a major issue for traditional insurance carriers. By design the internet is an interconnected mesh of nodes, ~~databases~~databases, and networks. There are many instances of cyberattacks hitting thousands of targets causing a meshed quagmire of losses[14]. The connected topology of the internet and corresponding nodes and databases are by nature interleaved. This creates a potential of mass loss due to two main factors; 1) large scale service providers (cloud platforms) used by millions of policy holders create potential for large scale claims issuance, 2) the potential for derivative loss to policy holders associated with subscribers, ~~clients, patients~~clients, patients, etc. that suffer loss as a product of automated attack proliferation.

The inability for the traditional insurance industry to accurately ~~pin-point~~pinpoint cyber risks also presents an
existential problem for carriers. Initially many cyber security insurance carriers used a common practice of "risk pooling". This is the practice of commingling risk across many policies across many lines of coverage(s) to spread risk across held policies and lines of coverage[15]. This proved to be ineffective as losses exceeded initial projections and threatened commingled lines of coverage. In September 2022 the industry petitioned the United States Federal Trade Commission through Request For Comments (RFC) responses made accommodations for insurance companies to build stand-a-lone models specific to cyber security risk. The FTC took a ~~hands off~~hands-off approach to allowing insurance carriers the ability to change cyber coverage on an as needed basis[16]. The FTC held Penn Treaty as an example of how inaccurate loss projections could have a devastating impact on individual companies and the industry as a whole[17].

The legal system has yet to resolve key questions pertaining to what ~~is actual cyber harm~~actual cyber harm is. At the center of this legal confusion is; 1) does exposure on to itself represent a hardened form of loss, or 2) does eminent loss due to exposure constitute loss? The Supreme Court of the United has refused to weigh in. SCOTUS denied a Writ of Certiorari when in **March 2019** in the matter of ***Zappos.com,* Inc. v. Stevens *Zappos*** (an Amazon subsidiary) contended mere loss of data did not constitute actual loss when that data was not used for "nefarious" activities[18]. ***Zappos*** was appealing a lower court ruling Zappos was liable. Uncertainty over standing in data breach litigation is important for cyber insurers because it directly affects the probability that an insurer will have to pay claims in the event of a data breach.

[13]. Cyber Insurance | Federal Trade Commission (ftc.gov)
[14] The top five cyber security incidents in June 2023 (cshub.com)
[15] Cybersecurity Insurance Has a Big Problem (hbr.org)
[16] Digital Services Strategy Presentation (treasury.gov)
[17] The risks of pricing new insurance products: The case of long-term care (researchgate.net)
[18] U.S. top court rejects shoe retailer Zappos appeal in data breach case | Reuters

[15]https://www.cyberseek.org/

At the heart of the insurance industry is the actuary process. Actuary ~~by definition is~~is the process whereby financial costs of risks are weighed against risk and uncertainty[19]. The tools of the trade are mathematics, historical ~~statistics~~statistics, and financial theories to assess the cost of potential events. In theory this cost is applied to policy development that mitigates the impact and cost of defined risks. This approach is effective when applied to traditional lines of insurance because there exists a robust historical cache of loss information; for example, a car insurance company can extrapolate eventual loss as there is rich and ~~long lasting~~long-lasting history of driver, road, geographic and age data to pull from in order to model losses. In cyber security insurance, policies are presented with ~~a number of~~several paradoxes prohibiting traditional loss modeling.

3.1.1 Paradox One – Lack of History

Cybercrime is a relatively new field compared to traditional lines of insurance. There is very little historical precedent to draw actuary or risk profiling[20]~~.~~. The SEC has taken the lead as of July 26th, ~~2023~~2023, by requiring SEC regulated companies to disclose within 96 hours any knowledge of cyber breaches by way of SEC filing 8-K[21]. The new requirements go further by requiring companies to report risk strategy, ~~management~~management, and governance in annual 10-K filings[21]. Going forward these new requirements will benefit the industry as a whole; however, as it stands today there remains little historical data.

3.1.2 Paradox Two – Awareness Gap – Client Preparedness

A recent study commissioned by IBM found 77% of enterprise level companies lacked a cohesive incident response plan[22]**.** An organizations' lack of knowledge about internal readiness for ~~cyber attacks~~cyber-attacks make underwriting exceedingly difficult for insurers.

3.1.3 Paradox Three – Cyber Attack – Lack of a Definition

According to NIST a cyber attack is, "***An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information~~";~~";*** however, a search on Cyber Infrastructure Security Agency (CISA)[23] indicates the definition of a cyber attack has more to do with intent than means. Even when considering NIST's definition there remains a huge gap in precise and accurate definitions for what a cyber attack is. Without clear and concise definitions of threats there will remain a misunderstanding of how cyber threats impact carriers and policy holders. Without codified definitions cyber insurance policies will lack efficacy in policy coverage.

3.1.4 Paradox Four – No Geographic Boundaries

Locations for cyber insurance coverage are undefined. Client data can reside on premise, private cloud, public cloud or in hybrid environments Cyber attacks can be initiated from anywhere. It is estimated approximately 60% of attacks utilized internal corporate resources; however, 55% were the cause of external initiation like phishing, malware, open access, etc[24]. The in-flight nature of data presents an issue for the application of a standard rule of law.

3.1.5 Paradox Five – Lack of Actuarial Knowledge

Actuarial~~y~~ review is the cornerstone of underwriting. Cyber insurance is fundamentally different from other types of coverage, and with a lack of traditional markers to establish a risk position there is almost no actuary process for policy structure. This presents an actuarial~~y~~ dilemma ~~i.e.~~i.e., if a company gets breached and responds strongly, is that company then more prepared and thus a better risk in the future? If so, can the insurer charge a lower premium for previously breached companies if their responses to those attacks have lowered future risks?

[19] Actuaries : Occupational Outlook Handbook: : U.S. Bureau of Labor Statistics (bls.gov)
[20] Data Deficit Remains Key Challenge for Cyber Insurance Underwriters (insurancejournal.com)
[21] SEC adopts cybersecurity disclosure rules (pwc.com)
[22] IBM Study: Responding to Cybersecurity Incidents Still a Major Challenge for Businesses (prnewswire.com)
[23] CISA | CISA
[24] 115 cybersecurity statistics + trends to know in 2023 (norton.com)

3.1.6 Paradox Six – Prevention VS. Insurance

There is a legitimate debate among organizations to either fund cyber security insurance, or to fund a better security posture. In a 2022 commissioned Talion survey 70% of United Kingdom CISO's stated the number of cyber attacks were exacerbated by ransom weare payouts from insurance carriers[25]. Adding to a growing sentiment that more resources be allocated to prevention as opposed to insurance are the following:

- Ransomware payouts are being scaled back, and may be illegal to pay due to a 2020 U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCEN) declared it illegal to pay ransom in some (most) cases as it was deemed to aid and benefit foreign adversaries of the United States[26]
- Policy exclusions are expanding; for example, acts of war, terrorism, foreign born attacks, etc. are a short list of exclusions.
- Scrutiny of post policy compliance. GenerallyGenerally, an insurance carrier issues a questionnaire. Many insurance questionnaires lack the knowledge of a cyber security subject matter expert; therefore, when a claim is filed carriers may introduce the need for the policy holder to publish framework compliance post claim filing.
- Lack of operational budget to deploy both an updated cyber security posture and cyber liability insurance[27].

The many variables impacting cyber insurance coverage and the dilemma of actually protectingprotecting and running a business has placed owners and C level management in a predicament as to how cyber risks should be addressed. The Government has created a framework for industry compliance with no discernable guiderails for the insurance carriers [28]. This has created an environment wheregovernmental agencies and insurance carriers are working in harmony to NOT insure policy holders.

[25] Blog | Ransomware | Cyber Insurance Debate (talion.net)
[26] Ransomware Advisory | Office of Foreign Assets Control (treasury.gov)
[27] How Much Should Your SMB Budget for Cybersecurity? (business.com)
[28] Encouraging Clarity in Cyber Insurance Coverage (oecd.org)

4.0 Solution Setting

4.1 Captive Insurance for Cyber Liability

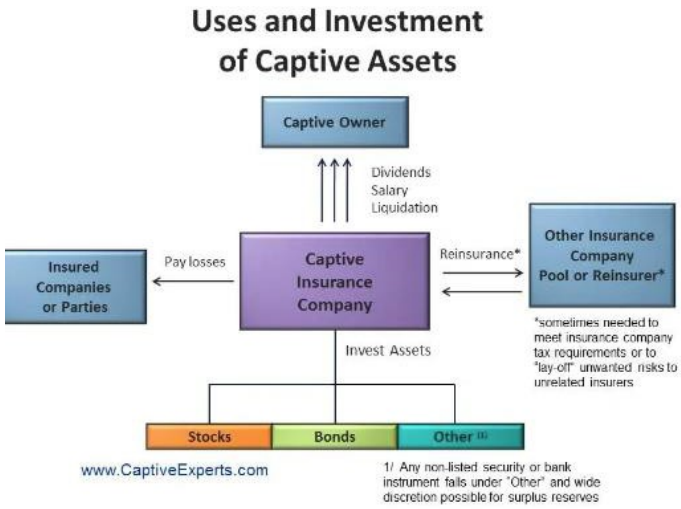
In 2021 AXA insurance company published an article titled, ***"The Road Less Travelled: Alternative Captive Uses"***[30]**.** The article was specific to the establishment of captive insurance companies ~~as a means to~~to meet the emerging risk of cyber security. In the ***Road Less Travelled*** AXA contends that premiums paid into a captive insurance company are more flexible for cyber security liability insurance when premiums can be utilized for customized policy language, regulatory compliance, pre and post breach remediation, and historical data incubation ~~as a means to~~to refine coverage over time.

Formatted: Highlight

Formatted: Highlight

By commuting ~~all of~~all the regulatory, tax and financial benefits associated with insurance coverage to the policy holder the captive model presents a powerful approach to meeting the needs specific to cyber security insurance. Captives create financial resources essential for a hybrid approach to mitigating cyber risks. Captives have been provided latitude to invest revenues associated with tax scheduling and premium surpluses. Many captives have established equity positions in ~~early stage~~early-stage tech, bridge funds, secondary business creations, etc[31]. Investment strategies are governed by state statutes from which the captive obtains its domicile license[31]**.** Many states have gone as far as to make published recommendations on captive investment structure and establishment of governance.

Source – Captive Experts - Captive Insurance Investments (captiveexperts.com)[31]



[29] Advantages of Captive Insurance | Department of Financial Regulation (vermont.gov)
[30] The road less travelled: Alternative captive use cases (axaxl.com)
[31] Captive Insurance Investments (captiveexperts.com)

4.2 Captive Insurance for Cyber Liability – Statement of Barriers

Barriers do exist for captive establishment. There is no industry accepted definition of what insurance ~~actually means~~means. In an article published for the *Connecticut Law Journal* in 2022 titled, ***"COMMONLY ACCEPTED NOTIONS OF INSURANCE" FOR CAPTIVES IN TAX CASES ARE NOT COMMON NOTIONS OF INSURANCE IN THE INSURANCE INDUSTRY*** Harold Weston (Clinical Associate Professor of Risk Management and Insurance, Georgia State University) writes:

"The insurance field allows multiple definitions to co-exist in a pragmatic and ~~highly regulated~~highly regulated marketplace. It is an ecosystem of regulations, law, theory, probabilistic mathematics, and economics. The tax courts, deciding tax deduction questions involving premiums paid to captive insurance companies, have settled on their own definition of insurance, which they call commonly accepted notions of insurance."

In ***COMMONLY ACCEPTED NOTIONS OF INSURANCE***, Weston asserts although there may not be homogeny on the definition of insurance, captives have clear structure and benefits from which insurance coverage imparts to policy holders. The lay person would apply the standard of "I know insurance when I see it". The earmarks of a captive established for nefarious reasons; for example, pure tax avoidance are[32]:

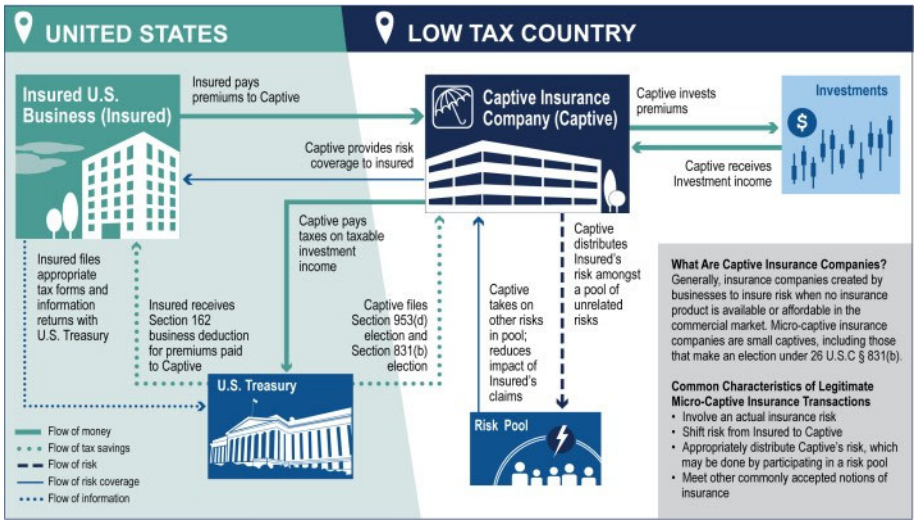
1. Lack of coverage feasibility
2. Ignorance of state tax laws
3. Single line focus
4. Poorly drafted or lack of structured policies
5. Poorly constructed insurance contracts
6. Captive is lacking capital and reinsurance~~e~~
7. Longshot risks – Inflated premiums vs. risk

In a landmark legal case in 2017 ***BENYAMIN AVRAHAMI AND ORNA AVRAHAMI, v. COMMISSIONER OF INTERNAL REVENUE*** the IRS won a decision where Benyamin ***Avrahami*** (strip mall owner) failed to meet the Commonly Accepted Notions of Insurance standard[33]**.** As a ~~result~~result, the beneficial tax schedule ***Avrahami*** was enjoying was revoked. The IRS contended ***Avrahami*** captive insurance company premiums soared from 150,000.00 annually to 1,500,000.00; ~~while,~~while not being able to show a discernable reason for the increase in premiums (***Avrahami*** reported no losses). Further, *Avraha*mi took personal loans from the captive insurance company and claimed tax deductions.

As a result of Avrahami in 2020 the United States Government Accountability Office (GAO) in its "***Report to the Chairman, Committee on Finance, U.S. Senate - ABUSIVE TAX SCHEMES - Offshore Insurance Products and Associated Compliance Risks***" took the opportunity to add light as to the validity of micro-captive insurance companies[34]**.** A micro-captive insurance company is formed with owners electing to be taxed on the captive's investment(s) only, not its underwriting profits. In the *Report to the Chairman* the GAO published the following diagram on the basic processes and handling of premiums paid. It was the recommendation of the GAO those captives that did not follow this basic model should be subject to IRS scrutiny[34].

[32] Commonly-Accepted-Notions-of-Insurance-Weston-CILJ-Vol.-28.1.pdf (uconn.edu)
[33] 149_TC_No_7.pdf (ustaxcourt.gov)
[34] GAO-20-589, ABUSIVE TAX SCHEMES: Offshore Insurance Products and Associated Compliance Risks

Source - GAO-20-589, ABUSIVE TAX SCHEMES: Offshore Insurance Products and Associated Compliance Risks[34]



The Avrahami Case combined with the GAO position statement provide clear reasoning for legitimate insurable risk when forming a captive ~~establishment is needed~~. The establishment of captive has prima facie validity when the impetus of the captive is structured to render insurance, not tax avoidance. Captives are a unique structure to meet the complexities in cyber security.

[32] Commonly-Accepted-Notions-of-Insurance-Weston-CILJ-Vol.-28.1.pdf (uconn.edu)
[33] 149_TC_No_7.pdf (ustaxcourt.gov)
[34] GAO-20-589, ABUSIVE TAX SCHEMES: Offshore Insurance Products and Associated Compliance Risks

4.3 Sponsored Captive – A Hybrid Approach

Traditional insurance carriers are ill equipped to understand the technological aspects of cyber threats. Cyber Security Insurance is in need of hybrid structures where the insurer understands the regulatory, legal and accounting associated with insurance coverage; while, understanding cyber threats through integrated technology and expertise to proactively remediate cyber threats. According to InfoSec, a leading United Kingdom Security Operations Center (SOC), cyber security insurance presents a crisis for the industry[35].

InfoSec quotes premiums have increased 94% from 2019 to 2022. Probably most shocking, loss runs in the industry ~~as a whole are~~are 60%[35]. Carriers have tightened policy language rendering coverage worthless. At some point cyber security insurance by traditional carriers will be uninsurable. This point was pronounced by Zurich CEO Mario Greco in December 2022 in an interview with The Financial Times[36].

Captives can be structured to cover everything from gap to primary lines of coverage[37]. ~~For the purpose of~~For cyber liability ~~insurance~~insurance, the focus will be placed on the concept of a "Sponsored captive" structure. A definition of a Sponsored captive can be found on the Vermont Department of Financial Regulation[38]. Vermont states:

A sponsored captive insurance company has its minimum capital and surplus provided by one or more qualified sponsors. The business of a sponsored captive may only insure the risks of participants through separate participant contracts, and the liability to each participant must be funded through one or more cells. ~~The assets~~The assets of cells ~~are available~~are available ~~only to~~only to satisfy the liabilities of that cell. Cells ~~are formed~~are formed as protected or incorporated protected.

By Vermont's definition, a sponsored captive policy holder may participate in a captive through sponsorship as an individual "cell"; while, not commingling liabilities and assets with other policy holders. This allows for policy holders to "right size" risk profiling along with insurance premiums based upon the specific metrics for cyber liability loss. Further, flexible coverage allows for the individual policy holders (cell) companies to take advantage of tax scheduling and freedom to invest premium surpluses.

Policy holders generally lack the expertise and resources to establish a captive insurance company and the technology and eco system to impact cyber protections. Management companies for captives have been around for many years, to the point where captive management is a mature industry. A captive management company, as defined by the International Risk Management Institute provide[39]:

- Serve as the primary contact with the domiciliary ~~regulators, and~~regulators and ensure compliance with all domicile regulations.
- Develop business plans and pro forma financial statements.
- Maintain the captive's financial and operational records.
- Provide insurance, risk management, and underwriting expertise to the captive.
- Provide quarterly and annual financial reports for the captive's owners and board of directors.
- Coordinate the captive's board meetings.

[35] The evolution of cyber insurance | JUMPSEC
[36] Cyber attacks set to become "uninsurable" suggests Zurich's Greco - Reinsurance News
[37] Captive Insurance Companies (naic.org)
[38] Become a Vermont Captive | Department of Financial Regulation
[39] 5 Key Attributes of Captive Managers
[40] Global Report: 2023 State of Threat Detection | Vectra AI
[41] NIST Risk Management Framework | CSRC
[42] USA Cyber Security Companies | CyberDB

- Serve as the main point of contact for the captive's service providers, including the actuary, auditor, claims administrator, broker, fronting insurer, investment adviser, and any other professional service providers.

The sponsored captive structure allows for a specialized type of captive manager to add technical value along with conventional captive management services. The sponsored captive manager ~~is able to~~can own, license and maintain cyber threat discovery tools. Cyber support eco systems are fostered leveraging the discovery of cyber threats specific to each policy holder. The ideal sponsored captive manager will have these foundational elements as a means to cross the chasm between insurance and technical knowledge in order to render complete; ~~yet,~~yet flexible cyber security policies with lower loss runs:

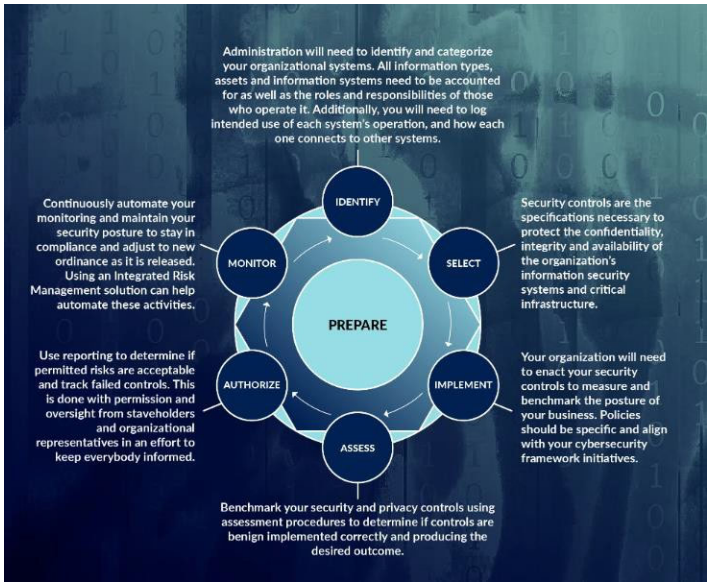
1. The sponsored captive insurance management company itself will need a well structured reinsurance~~e~~ policy in order to distribute the potential catastrophic loss of one cell. Reinsurancee policy will need to be underwritten as predictive loss, not on historical loss run analysis.
2. Strong foundation in cyber security technology. Specific areas of competence are in cyberthreat discovery. In the most recent **2023 State of Threat Detection** published by Vectra (an artificial intelligence repository for cyber security incidents) 90% of Security Operations Analysts felt current detection tools were effective in locating cyber threat vectors[40]. According to the United States Federal Agency Cybersecurity and Infrastructure Security Agency (CISA) 92% of attacks can be avoided by patching.

3. Cyber security engineering personnel. The engineer function will be to normalize discovery data with policy holders and IT staff. Engineers will aid policy holders through the sponsored captive manager eco system for precise and fast recommendations on subject matter expertise for remediation of any discovered threats.

4. Eco System of professional services firms. The sponsored captive manager will act as a technological security blanket to augment policy ~~holders~~holders' personnel. Threat discovery will be relayed to the policy holder within the NIST six essential steps to Risk Assessment[41]:
    1. Categorize Information Systems
    2. Select Security Controls
    3. Implement Security Controls
    4. Assess Security Controls Authorize Information Systems
    5. Authorize Information Systems
    6. Monitor Security Controls

[35] The evolution of cyber insurance | JUMPSEC
[36] Cyber attacks set to become "uninsurable" suggests Zurich's Greco - Reinsurance News
[37] Captive Insurance Companies (naic.org)
[38] Become a Vermont Captive | Department of Financial Regulation
[39] 5 Key Attributes of Captive Managers
[40] Global Report: 2023 State of Threat Detection | Vectra AI
[41] NIST Risk Management Framework | CSRC
[42] USA Cyber Security Companies | CyberDB

Source of Image: The Six Steps of the NIST Risk Management Framework (RMF) (cybersaint.io)



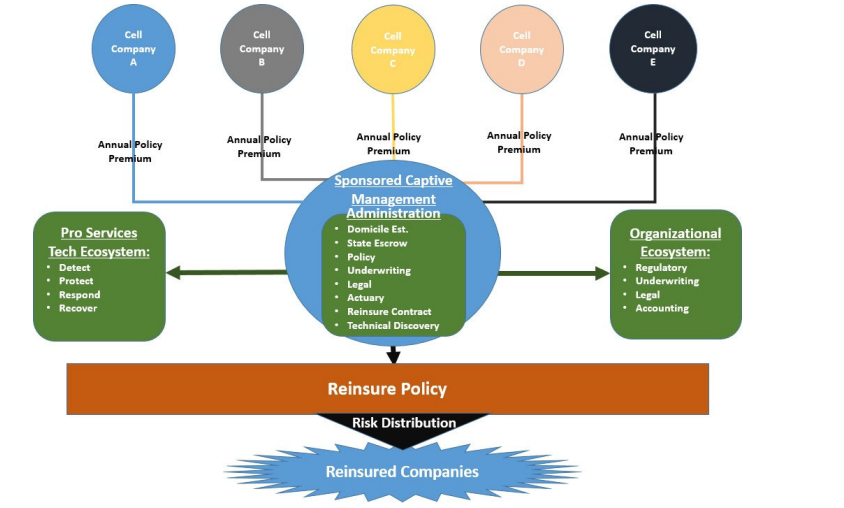
5. SaaS based discovery. The NIST Risk Management Framework (RMF) can be accomplished via ~~software based~~software-based discovery tools. The sponsored captive manager will encapsulate these services in Software as a Service (SaaS) platform. Constant threat detection is required, deploying a SaaS discovery enables policy holder support teams to focus efforts in relation to the NIST 2.0 Framework; and, draws in policy holder senior leadership for governance of cyber security by outlining cyber protection prioritization.

6. Maintain a Roster of eco system affiliates based on function and competencies. According to CyberDB (a cyber research data bank) as of 2023 there are over 3,500 companies focusing on cyber security services[42]. Cyber security professional services are becoming specialized to specific cyber remediation activities. The sponsored captive manager will build a data base of cyber remediation companies and areas of expertise in order to assist with policy ~~holders~~holders' cyber remediation needs.

7. The proposed sponsored captive manager as diagramed below:

[35] The evolution of cyber insurance | JUMPSEC
[36] Cyber attacks set to become "uninsurable" suggests Zurich's Greco - Reinsurance News
[37] Captive Insurance Companies (naic.org)
[38] Become a Vermont Captive | Department of Financial Regulation
[39] 5 Key Attributes of Captive Managers
[40] Global Report: 2023 State of Threat Detection | Vectra AI
[41] NIST Risk Management Framework | CSRC
[42] USA Cyber Security Companies | CyberDB

Proposed Sponsored Captive Insurance Company~~Manager~~ Structure Diagram



[35] The evolution of cyber insurance | JUMPSEC
[36] Cyber attacks set to become "uninsurable" suggests Zurich's Greco - Reinsurance News
[37] Captive Insurance Companies (naic.org)
[38] Become a Vermont Captive | Department of Financial Regulation
[39] 5 Key Attributes of Captive Managers
[40] Global Report: 2023 State of Threat Detection | Vectra AI
[41] NIST Risk Management Framework | CSRC
[42] USA Cyber Security Companies | CyberDB

5.0 Summary

Sponsored captive insurance companies allow for a unique method to address policy holder cyber security insurance. Sponsored captives may utilize management firms to assist in the establishment of captive legal, accounting, regulatory and governance. Most importantly sponsored captives can offer additional services ~~in the area of~~in cyber security.

Cyber security insurance presents many problems for actuary and underwriting as evidenced by 60% loss runs. The lack of discernable historical data, attack sophistication, broadening of compute surface space does not fit well into the conventional insurance risk model. The cyber security insurance industry ~~is in need of~~needs hybrid coverage that addresses risk mitigation and cyber threat remediation quantified in a predictive model.

Sponsored captive insurance management renders an environment where insurance and cyber knowledge meet so policy premiums cover actual risk. Further, policy holders are provided fiscal benefits through tax scheduling and surplus return. Monetary surpluses created by tax scheduling and low loss run can be invested to deploy internal personnel and controls for cyber security protection.

By having expertise in captive organization and cyber threat discovery the sponsor captive manager, will act as a "toggle" where captive eco systems (legal, actuary, accounting, reinsure, governance) and technical ecosystems (cyber threat discovery and remediation) can be managed under a single entity.

The sponsored captive insurance company model also allows for a fundamental change in actuary analytics. By focusing on ~~discovery~~discovery, the sponsored captive manager can use a pure predictive loss model, not a historical loss model. Applying predictive algorithmic analytics to threat vectors and compared to cyber security preparedness will yield better historical data and lower loss for future policy holders. By initiating complete external and internal compute discovery, executing a comprehensive NIST Framework remediation plan supported by cyber security governance 98% of attack surface area can be secured. Extrapolated over 1,000 sponsored captives, the loss run would be below 20%, this is a 200% improvement over current traditional insurance model loss ~~runs~~runs.