Recorded Future®

A New Cyber Insurance Model: Continuous Control Validation

By Levi Gundert

Abstract

Can private-sector cyber insurers accurately understand and price risk? This paper analyzes the current state of the cyber insurance market and offers a new framework for insurers to evaluate risk. Cyber insurance is a nascent market and cyber insurers have already experienced significant losses from ransomware attacks, leading to fewer options for private-sector coverage. This trend is counterproductive to the public interest. As businesses struggle to defend themselves against malicious actors with significant resources, insurance plays an increasingly critical role in risk mitigation strategy and even the health of national economies.

Structure

In this paper, I discuss the current state of the cyber insurance market. I then dissect current insurance policy loss causation, including an over-emphasis on attack attribution and a lack of underwriting rigor exacerbated by infrequent customer control audits. Next, I detail a risk model based on adversary tactics and continuous control validation while borrowing from auto policy telematics (and connected privacy considerations) to frame a new type of partnership between insurers and the insured toward a healthier cyber insurance market.

Table of Contents

Introduction

Insurance is a historical method for limiting risk that dates to the ancient world[1]. Few modern-day objects[2] or events are incapable of insurance coverage — insurance companies have devised policies for personal[3] (home, auto, life, umbrella) and commercial[4] (lawsuits, employee injury, unexpected events) coverage to reduce the probability of monetary loss. However, consumer choice in private insurance markets requires a profitable business model. Accordingly, insurance companies have determined profitable formulas for pricing risk[5] that are codified in actuarial tables[6].

Conversely, cyber insurance policies have proven difficult to appropriately price, as evidenced by mounting insurance industry losses[7]. Cyber insurance emerged at the end of the twentieth century, and demand for coverage accelerated in the first two decades of the twenty-first century[8] as cyber threats matured and proliferated. Most recently, ransomware as a service has emerged as an exceptionally successful[9] monetization model for cybercriminals, driving increased demand for risk mitigation strategies that include cyber insurance.

Thomas Johansmeyer, associate vice president of property claim solutions at Verisk Insurance, encapsulates the current situation: “So, prices are low, and the risk is high. This dynamic has negatively influenced the market’s ability to continue to grow at its previous aggressive rate — and has led to a profound shortage of cyber insurance[10]”. My own interviews with an insurance broker, insurers, and Recorded Future[11] clients confirm that the cyber insurance market is aggressively contracting. Businesses are facing significantly higher premiums to obtain and renew cyber insurance policies with coverage parity. One company shared the prospect of employing 10 different insurers to renew a policy with $100 million of aggregate coverage. Demand is superseding available supply as insurers exit the market[12].

[1] (History of insurance)

[2] (McLachlan, 2021)

[3] (Types of Personal Insurance Coverage)

[4] (Insurance for Your Business Made Simple)

[5] (Facts + Statistics: Auto insurance)

[6] (Social Security Actuarial Life Table)

[7] (Cyber Insurance Losses Spark Rate Increases, 2021)

[8] (Morris)

[9] (Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021, 2021)

[10] (Johansmeyer T. , 2020)

[11] (The Recorded Future Platform, n.d.)

[12] (Johansmeyer T. , 2021)

The US General Accountability Office confirmed these trends, saying,

> The extent to which cyber insurance will continue to be generally available and affordable remains uncertain. Despite the upward trend in take-up rates to date, insurer appetite and capacity for underwriting cyber risk has contracted more recently, especially in certain high-risk industry sectors such as health care and education for the public-sector entities, according to the Council of Insurance Agents and Brokers, Marsh McLennan, and A.M. Best[13].

Losing access to private market cyber insurance is a threat to businesses and a disservice to the public interest, similar to the loss of personal flood[14] or fire[15] coverage in disaster-prone areas. Even if governments must intervene with additional capital (becoming the insurers of last resort) or improved governance[16], taxpayers deserve a better model for insuring cyber risk. Certainly, reinsurers play a significant role in market liquidity, but even they face "structural challenges and systemic risks, the increase in cyber-attacks, and an accumulation of exposures… [including] the non-affirmative exposures we refer to as 'Silent Cyber.'[17]"

The risks remain opaque for insurers and reinsurers due to the difficulty with international cyberattack attribution[18] and the complexity of technical business operating environments. Further, technical control efficacy frequently changes, leaving point-in-time assessments[19] lacking and traditional underwriters dependent on third-party auditing services[20] that provide only partial exposure visibility. An improved underwriting model is required to restore insurer faith in risk exposure and expand the global cyber insurance market to the benefit of the global economy.

[13] (Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market, 2021)

[14] (Congress, 2014)

[15] (Zip Codes Covered by Mandatory One Year Moratorium on Non-Renewals, n.d.)

[16] (Cunningham & Talesh, 2021)

[17] (Cyber Risks In A New Era: Reinsurers Could Unlock The Cyber Insurance Market, 2021)

[18] (Clarke, 2020)

[19] (McKenna, 2018)

[20] (BitSight Security Ratings, n.d.)

Cyber Insurance Underwriting Challenges

The 2020 Cyber Solarium Commission opined that "the market for insurance must accurately price risk[21]". In the following section, I detail the need for underwriters to consistently access and interpret stream analytics in order to rigorously evaluate cyber risk and iteratively adjust policy ratings and pricing. Proper analytics need to address both historical loss amounts and the security state of the insured at any point in time.

The past decade has created a critical mass[22] of insured and uninsured loss amounts now available for underwriters to reference. While comprehensive data equal to life or auto policies is still elusive, underwriters can reference open-source historical data on losses from operational downtime, regulatory penalties, remediation and services, ransomware payments, ransomware negotiation services, and more.

Equally important to understanding previous losses is crafting policies with prescriptive verbiage that removes ambiguity and reduces the probability of future protracted[23] legal conflict. According to Woodruff Sawyer, "Insurers are now communicating more explicitly about what types of events can trigger a cyber policy, and what losses the policy pays out[24]".

An analysis of 2017 to 2019 generic cyber policy templates from Chubb, Axa, Zurich, and Beazley reveals issues when applied to the cyber domain. For example, one insurer defines the "War" policy exclusion as:

> ...Strikes or similar labor action, war, whether declared or not, invasion, act of foreign enemy, civil war, mutiny, coup d'état, civil commotion assuming the proportions of or amounting to a popular rising, military rising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against these actions; provided, however, this exclusion shall not apply to any actual, alleged or threatened attack against the network, with the intention to cause harm to further social, ideological, religious or political objectives or to intimidate any person or entity in furtherance of such objectives.

[21] (King & Gallagher, 2020)

[22] (Cyber Security Case Studies, n.d.)

[23] (Corcoran, 2019)

[24] (Chen, Get Ready: Cyber Insurance Underwriting is Changing, 2020)

The inclusion of “religious or political objectives” as an exclusion carve out raises questions about cyber actions originating in countries where government employees[25], proxies[26], contractors[27], or even semi-autonomous actors[28] motivated by illicit revenue are directly or indirectly advancing a national purpose. A different insurer defines “Act of Cyber-Terrorism” similar to the definition of “War” given above:

> Act of Cyber-Terrorism means: (i) any act, including force or violence, or the threat thereof, expressly directed against a Computer System operated by an Insured, by an individual or any group or individuals, whether acting along, on behalf of or in connection with any entity or government to damage, destroy, or access a Computer System without authorization; or, (ii) a targeted denial of service attack or transmittal of corrupting or harmful software code at or into the Insured’s Computer System for social, ideological, religious, economic or political reasons, including intimidating or coercing a government, a civilian population or disrupting any segment of an economy.

Does ransomware meet the definition of “damage” when data is inaccessible but systems remain available? Insurer policy template language raises more questions and contributes to ambiguity[29] when focused on attack attribution. The Tallin Manual[30] attempts to summarize current international law and cyberspace norms. While the work is important toward cyber peace efforts, insurers must press onward with clear policy language for negative cyber event coverage regardless of attack attribution.

[25] (Insikt Group, 2021)

[26] (Gundert, Chohan, & Lesnewich, Iran’s Hacker Hierarchy Exposed, 2018)

[27] (Insikt Group, 2017)

[28] (Insikt Group, 2021)

[29] (Bershidsky, 2019)

[30] (Jensen, 2018)

Certainly, insurers will continue to define attack attribution carve-outs to limit damages, as the 2017 NotPetya[31] attacks illustrated in the now infamous Mondelez International, Inc. v. Zurich American Insurance Company case (the case was filed in 2018 and a final disposition appears elusive in the foreseeable future).[32] NotPetya also led to Merck's[33] ongoing litigation against Allianz SE and American International Group Inc. on a property and casualty policy[34] claim that centers on whether NotPetya was an "Act of War". Insurance policies should be crafted to avoid lengthy litigation by focusing on technical control failure causation and less on the actor(s) originating the attack because attribution is often the domain of intelligence agencies and attempting to divine motivations is unproductive both for insurers and the insured seeking first-party coverage.

Finally, underwriters need technical assistance from subject matter experts[35] and constant analytics derived from a proposed insured's systems and network. Allstate[36] and Lemonade[37] recently announced their desire for near real-time vehicle telematics to more accurately price risk in auto policies. Cyber policy underwriters need access to similar telemetry from both internal and external sources to understand risk more accurately. While attestations have historically played a key role in underwriting, they are not sufficient to determine a proposed insured's cyber defenses or, more importantly, operational resilience. Similarly, infrequent audits (for example, quarterly) are insufficient to measure control[38] efficacy when adversary tools and tactics evolve daily.

[31] (Nakashima, 2018)

[32] (Rand)

[33] (Voreacos, Chiglinsky, & Griffin, 2019)

[34] (De Azevedo & Kasper, 2021)

[35] (Chen, Get Ready: Cyber Insurance Underwriting is Changing, 2020)

[36] (Scism, Allstate Wants to Track Your Driving to Determine Your Car Insurance Rate, 2021)

[37] (Scism, Insure-Tech Firm Lemondade to Offer Car Insurance, 2021)

[38] (Kenneally, 2021)

A New Model: Continuous Control Validation

In the following section, I detail a new type of framework for cyber insurance policy evaluation that more accurately reflects risk.

In 2018, Warren Buffet opined[39], "Frankly, I don't think we or anybody else really knows what they're doing when writing cyber. People who say they have a firm grasp on the risk are kidding themselves." Indeed. Solutions are needed, as stated by New York's Department of Financial Services when it released its 2021 Cyber Insurance Risk Framework[40]. The seven-point guide is a valuable start for insurers. However, point 4 — "Rigorously Measure Insured Risk" — requires a more rigorous assessment process.

> Insurers that offer cyber insurance should have a data-driven, comprehensive plan for assessing the cyber risk of each insured and potential insured. This commonly starts with gathering information regarding the institution's cybersecurity program through surveys and interviews on topics including corporate governance and controls, vulnerability management, access controls, encryption, endpoint monitoring, boundary defenses, incident response planning and third-party security policies. The information should provide a detailed picture, enough for the insurer to make a rigorous assessment of potential gaps and vulnerabilities in the insured's cybersecurity. Third-party sources, such as external cyber risk evaluations, are also a valuable source of information. This information should be compared with analysis of past claims data to identify the risk associated with specific gaps in cybersecurity controls.

The successful implementation of New York's framework depends on the speed and volume of "information gathering." Surveys and attestations are helpful for underwriters to begin gauging administrative and process controls, but technical control evaluation should begin with continuously testing controls against threat actor tools and techniques.

Even the US Department of Commerce's National Institute of Standards and Technology (NIST) Cybersecurity Framework's[41] (CSF) five phases — Identify, Protect, Detect, Respond, Recover — are helpful to structure the underwriting process and identify gaps in implementation. Still, risk mitigation success relies on a detailed and rigorous inspection of each category. For example, ID.RA-3 states, "Threats, both internal and external, are identified and documented." Underwriters must understand the types of threats and the market data available to satisfy a framework requirement. Are the prospective insured programmatically collecting stolen employee credentials and proactively resetting passwords where necessary? How long does it take an enterprise to patch remote code execution vulnerabilities? What is the phishing simulation success rate? These are the types of questions that require iterative and consistent analytics, not attestations.

[39] (Griffin, 2019)

[40] (New York Department of Financial Services, 2021)

[41] (Commerce, 2018)

Underwriters should adopt a threat taxonomy[42] that is flexible and practical, focusing on initial unauthorized access methodologies and the subsequent harm that may result to systems and data. For example, Recorded Future research[43] detailing a threat actor's playbook for establishing unauthorized access found it largely revolves around three techniques: credential reuse, remote code exploits for known vulnerabilities, and phishing. These tactics are not exhaustive (supply chain[44] issues[45] and third-party vendor connectedness also present challenges[46]), but they represent a disproportionate amount of successful unauthorized access.

Underwriters need ongoing telemetry-based analytics from the proposed insured to better understand how security controls are faring for each threat category. While the insured may be loath to share internal data with insurers, if the relationship becomes a partnership toward improved security, then both parties benefit from reduced risk and less revenue lost. In the same way that private equity firms advise portfolio companies, insurance companies should partner with their clients for risk management success.

For example, sharing phishing test[47] success and failure analytics would provide an underwriter one metric to measure employee education campaign effectiveness. Over time the insurer could share best practices among clients and help improve phishing test results. Similarly, sharing technical control analytics[48] from email security gateways would help insurers better understand the likelihood of an attacker evading the control in question.

Another example of shared protective control visibility is the recovered authentication credentials stolen via either third-party database compromise or malicious code ("malware"). Comprehensive multi-factor authentication (MFA) requires validation beyond attestation, particularly the process and time required to add MFA to new systems and applications along with daily updated electronic asset inventories. Beyond the iterative technical control validation, insurers need identity analytics from intelligence-derived stolen credentials. Sharing the weekly number of valid recovered credentials provides an additional analytic that signals a prospective customer's commitment to reducing the potential for malicious credential reuse.

Finally, timely vulnerability management is a critical capability to prevent cyberattacks. Modern enterprises are faced with the daunting task of managing significant technical complexity in systems and applications, often including fragile legacy systems, internet-of-things (IoT) devices, and operational technologies (OT). Instead of focusing on broad program availability, insurers should focus on the time needed to remediate more manageable numbers of remote code execution (RCE) vulnerabilities that lead to the largest loss scenarios like ransomware (bad actors deploying ransomware targeted forty-five vulnerabilities in Q2 and Q3 2021 according to Recorded Future research[49]).

[42] (Gundert, The Risk Business - What CISOs Need to Know About Risk-Based Cybersecurity, 2020)

[43] (Insikt Group, 2019)

[44] (Aguirre, 2021)

[45] (Sharma, 2021)

[46] (Insikt Group, 2019)

[47] (caniphish, 2021)

[48] (RIces, 2021)

[49] (Insikt Group, 2021)

Following initial unauthorized access in victim networks, threat actors destroy data confidence, integrity, or availability. Cyberattacks, including social engineering, business email compromise (BEC), ransomware, personally identifiable information (PII) theft, and trade secret theft are often achieved using open-source tools.[50] Recorded Future research named the top ten "tools" used in 2020 cyberattacks: Cobalt Strike[51], Metasploit[52], PupyRAT[53], Powershell Empire[54], Meterpreter[55], Covenant[56], Armitage[57], Octopus[58], Responder[59], PoshC2[60]. Even closed-source tools[61] cost only a nominal fee (for example, per Recorded Future's Insikt Group, in October 2021, Mars Stealer was advertised in online markets for $160).

Continuous control validation against new tools and tactics is equally important for both phases of an attack life cycle — obtaining unauthorized access and performing malicious actions after gaining access. To evaluate controls first requires awareness of new adversary tools. Again, insurers should avoid attestations to the existence of intelligence or control validation programs and instead require control validation results that detail the process and results. In 2019 a cyber intrusion that included the Silent Trinity[62] open-source attack tool victimized[63] the Croatian government. Also in 2019, open-source Pupy[64] RAT maintained persistence inside a European energy sector organization.

Open source "red team tools" are attractive to both criminals and nation-state-sponsored adversaries because the tools obfuscate attack attribution efforts. Based on the Recorded Future intelligence platform, companies are victimized daily using these known toolsets. For insurers, checking for the presence of anti-virus and endpoint detection (EDR/XDR) software on a prospective customer's systems is relevant, but the deeper ability to mitigate risk lies in the ability to perform continuous control validation (either manually or using automation[65]) using the same tool sets that threat actors are daily using with disappointing success. Quarterly penetration tests or red team audits provide helpful visibility into control gaps, but threat actors' tools and tactics constantly evolve because the available free attack resources change daily. Control validation frequency in insured networks must keep pace.

[50] (Insikt Group, 2021)

[51] (Systems, 2021)

[52] (Rapid7, 2021)

[53] (n1nj4sec, n1nj4sec / pupy, 2021)

[54] (EmpireProject, 2021)

[55] (Rapid7, 2021)

[56] (Cobb, 2021)

[57] (rsmudge, 2021)

[58] (mhaskar, 2021)

[59] (SpiderLabs, 2021)

[60] (nettitude, 2021)

[61] (Insikt Group, 2021)

[62] (byt3bl33d3r, 2019)

[63] (Cimpanu, 2019)

[64] (n1nj4sec, Pupy, 2019)

[65] (AttackIQ Platform, 2021)

Telematics and Privacy

Legal questions related to telematics surface under recently implemented privacy legislation, including the European Union's General Data Protection Regulation[66] (GDPR) and California's Consumer Privacy Act (CCP). Needed control telemetry may contain GDPR-defined personal data (for example, IP addresses[67] or employee resource credentials), which necessitates creating telemetry-based derivative analytics that remove personal data and enable the insured to provide data-sharing transparency[68] for customers.

Future legislation and legislative revisions should consider the importance of data analytic availability for insurer review, understanding that insurers need derivative analytics, not necessarily raw telemetry that may include protected communications or content. Additionally, analytic transparency around sourcing origination and production will build trust and confidence in reliable signals for calculating risk.

Threat Category Risk

As previously discussed, continuous control validation sets a baseline for insurers and the insured to partner on risk mitigation strategies. Insurers should tailor cyber policies with more precise language to match desired risk exposure in one or more threat categories expanding granularity on the below matrix:

Initial Unauthorized Access Mechanism	Post-Compromise Activities
• Social Engineering • Credential Reuse • Known Vulnerabilities • Zero-Day Vulnerabilities • Misconfigurations • Protocol Hijacking • Physical Tampering • Rogue Employee	• Extortion • PII Theft • Trade Secrets Theft • Communications Theft • System or Data Harm or Destruction • Financial Fraud • Data Impairment

Insurers are removing ransomware coverage[69] from new cyber policies. Moving away from comprehensive cyber coverage and focusing on specific threat categories will reduce insurer exposure and help ensure that insurers better understand the risks for each category.

[66] (European Commission, 2018)

[67] (MISP, 2018)

[68] (California Consumer Privacy Act (CCPA), 2018)

[69] (Ikeda, 2021)

Conclusion

The existing market for cyber insurance is changing as insurers sustain heavy financial losses — imposed primarily by ransomware attacks — and businesses seek protection. The current lack of rigor in cyber policy underwriting is unsustainable, but improved risk evaluation is possible. Underwriters need deep technical resources and clients that function as risk partners to assess technical controls accurately.

Telemetry-derived analytics will help insurers increase threat visibility, and regulatory regimes should support efforts that balance privacy with sensible visibility for underwriters in the same way that insurers wish to obtain telematics from vehicles to assess auto policy risk. Finally, frequent and iterative control validation in customer environments is a requirement that insurers can ill afford to ignore. A proper understanding of threat categories and adversary toolkits will help underwriters decide which risks are acceptable.

A robust private sector cyber insurance market is worth saving to support businesses already challenged to operate in an asymmetric, hostile digital environment where criminals and foreign governments ransack and pillage. A more rigorous cyber policy underwriting process combined with more precise policy language, focused less on attack attribution and more on threat categories and tools, can help insurers thrive.

References

Aguirre, J. (2021, October 27). Fake npm Roblox API Package Installs Ransomware and has a Spooky Surprise. Retrieved from Sonatype: https://blog.sonatype.com/fake-npm-roblox-api-package-installs-ransomware-spooky-surprise

AttackIQ Platform. (2021). Retrieved from AttackIQ: https://attackiq.com/platform/

Bershidsky, L. (2019, January 10). The Danger of Calling Out Cyberattackers. Retrieved from Bloomberg Opinion: https://www.bloomberg.com/opinion/articles/2019-01-11/mondelez-lawsuit-shows-the-dangers-of-attributing-cyberattacks

BitSight Security Ratings. (n.d.). Retrieved from BitSight: https://www.bitsight.com/security-ratings

byt3bl33d3r. (2019). Silent Trinity. Retrieved from GitHub: https://github.com/byt3bl33d3r/SILENTTRINITY

California Consumer Privacy Act (CCPA). (2018). Requests To Know Personal Information. Retrieved from State of California Department of Justice: https://www.oag.ca.gov/privacy/ccpa#sectionc

caniphish. (2021). Retrieved from caniphish: https://caniphish.com/

Chen, E. (2020, April 30). Get Ready: Cyber Insurance Underwriting is Changing. Retrieved from Woodruff Sawyer: https://woodruffsawyer.com/cyber-liability/cyber-insurance-underwriting-changes/

Chen, E. (2020, April 30). Get Ready: Cyber Insurance Underwriting is Changing. Retrieved from Woodruff Sawyer Insights: https://woodruffsawyer.com/cyber-liability/cyber-insurance-underwriting-changes/

Cimpanu, C. (2019, July 5). Croatian government targeted by mysterious hackers. Retrieved from ZDNet: https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

Clarke, D. T. (2020). Cyber Warfare and the Act of War Exclusion. Insurance & Reinsurance 2020, 11-15.

Cobb, R. (2021). Covenant. Retrieved from GitHub: https://github.com/cobbr/Covenant

Commerce, U. D. (2018, April 16). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from National Institute for Standards and Technology: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Congress, 1. (2014, March 3). H.R.3370 - Homeowner Flood Insurance Affordability Act of 2014. Retrieved from Congress.gov: https://www.congress.gov/bill/113th-congress/house-bill/3370

Corcoran, B. (2019, March 8). What Mondelez v. Zurich May Reveal About Cyber Insurance in the Age of Digital Conflict. Retrieved from LAWFARE: https://www.lawfareblog.com/what-mondelez-v-zurich-may-reveal-about-cyber-insurance-age-digital-conflict

Cunningham, B., & Talesh, S. A. (2021, May 20). Uncle Sam RE: Improving Cyber Hygiene and Increasing Confidence in the Cyber Insurance Ecosystem via Government Backstopping. Retrieved from SSRN.com: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3846435

Cyber Insurance Losses Spark Rate Increases. (2021, May 26). Retrieved from Fitch Ratings: https://www.fitchratings.com/research/insurance/cyber-insurance-losses-spark-rate-increases-26-05-2021

Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market. (2021, May). Retrieved from United States Government Accountability Office: https://www.gao.gov/assets/gao-21-477.pdf

Cyber Risks In A New Era: Reinsurers Could Unlock The Cyber Insurance Market. (2021, September 29). Retrieved from S&P Global Ratings: https://www.spglobal.com/ratings/en/research/articles/210929-cyber-risks-in-a-new-era-reinsurers-could-unlock-the-cyber-insurance-market-12118547

Cyber Security Case Studies. (n.d.). Retrieved 10 16, 2021, from Cyber Security Case Studies: https://www.cybersecuritycasestudies.com/

De Azevedo, C., & Kasper, D. (2021, May 4). 2021 Cyber Law & Regulation Outlook. Retrieved from Cyber Economics: https://www.cyber-economics.com/2021/05/04/2021-cyber-law-regulation-outlook/#zp-ID-1918-2414728-IQ52JP4M

EmpireProject. (2021). Retrieved from GitHub: https://github.com/EmpireProject

European Commission. (2018). Data protection in the EU. Retrieved from European Commission: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

Facts + Statistics: Auto insurance. (n.d.). Retrieved from Insurance Information Institute: https://www.iii.org/fact-statistic/facts-statistics-auto-insurance

Griffin, R. (2019, December 3). Merck cyberattack's $1.3 billion question: Was it an act of war? Retrieved from Bloomberg: https://www.inquirer.com/wires/bloomberg/merck-cyberattack-20191203.html

Gundert, L. (2020, January 1). The Risk Business - What CISOs Need to Know About Risk-Based Cybersecurity. Retrieved from Cyber Edge: https://cyber-edge.com/resources/the-risk-business/download/

Gundert, L., Chohan, S., & Lesnewich, G. (2018, May 9). Iran's Hacker Hierarchy Exposed. Retrieved from Recorded Future: https://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf

History of insurance. (n.d.). Retrieved from Baylor Blogs: https://cpb-us-w2.wpmucdn.com/blogs.baylor.edu/dist/a/6818/files/2013/12/History-of-insurance-11gcwej.pdf

Ikeda, S. (2021, May 13). France's Largest Insurer Will No Longer Cover Ransomware Payments. Retrieved from CPO Magazine: https://www.cpomagazine.com/cyber-security/frances-largest-insurer-will-no-longer-cover-ransomware-payments/

Insikt Group. (2017, May 17). Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3. Retrieved from Recorded Future: https://www.recordedfuture.com/chinese-mss-behind-apt3/

Insikt Group. (2019, February 6). APT10 Targeted NorwegianMSP and US Companies in Sustained Campaign. Retrieved from Recorded Future: https://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf

Insikt Group. (2019, October 30). Your Organization's Network Access is King: Here's What to Do About It. Retrieved from Recorded Future: https://www.recordedfuture.com/network-access-analysis/

Insikt Group. (2021, January 7). ADVERSARY INFRASTRUCTURE REPORT 2020: A DEFENDER'S VIEW. Retrieved from Recorded Future: https://go.recordedfuture.com/hubfs/reports/cta-2021-0107.pdf

Insikt Group. (2021, February 28). China-linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions. Retrieved from Recorded Future: https://www.recordedfuture.com/redecho-targeting-indian-power-sector/

Insikt Group. (2021, September 9). Dark Covenant: Connections Between the Russian State and Criminal Actors. Retrieved from Recorded Future: https://go.recordedfuture.com/hubfs/reports/cta-2021-0909.pdf

Insikt Group. (2021, August 31). H1 2021: Malware and Vulnerability Trends Report. Retrieved from Recorded Future: https://go.recordedfuture.com/hubfs/reports/cta-2021-0831.pdf

Insikt Group. (2021, October 28). Mars Stealer. Retrieved from Recorded Future: https://app.recordedfuture.com/live/sc/2s1dqgsNeRHq

Insurance for Your Business Made Simple. (n.d.). Retrieved from techinsurance.com : https://www.techinsurance.com/insurance-terms/commercial-insurance

Jensen, E. T. (2018, May 21). The Tallinn Mnaul 2.0: Highlights and Insights. Retrieved from Georgetown Law Internal Law Journal: https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf

Johansmeyer, T. (2020, October 9). Cyber insurance is only a few claims away from disaster. This is why it matters. Retrieved from World Economic Forum: https://www.weforum.org/agenda/2020/10/there-s-not-enough-money-in-cyber-insurance/

Johansmeyer, T. (2021, January 11). Cybersecurity Insurance Has a Big Problem. Retrieved from Harvard Business Review: https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem

Kenneally, E. (2021). The Role of Law and Government in Cyber Insurance Markets. University of Connecticut Insurance Law Journal. Retrieved from https://poseidon01.ssrn.com/delivery.php?ID=794089007091011095125107030007102077042014005059003070089127116007022024099103094097107039057104056039007122119009096064066001025010090051067093127023102065113011093026035120123088066022002004087012007081073112O

King, A., & Gallagher, M. (2020). Cyberspace Solarium Commission. Washington D.C.: U.S. Congress. Retrieved October 16, 2021, from https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view

McKenna, F. (2018, December 20). Unit of Equifax's auditor EY certified the information security that was later breached. Retrieved from Market Watch: https://www.marketwatch.com/story/unit-of-equifaxs-auditor-ey-certified-the-information-security-that-was-later-breached-2018-12-20

McLachlan, N. (2021, July 16). 11 of the Most Unusual Things People Have Ever Insured. Retrieved from US Insurance Agents: https://www.usinsuranceagents.com/unusual-insurance-policies/

mhaskar. (2021). Octopus. Retrieved from GitHub: https://github.com/mhaskar/Octopus

MISP. (2018, January 30). Information Sharing and cooperation enabled by GDPR. Retrieved from MISP - Open Source Threat Intelligence Platform: https://www.misp-project.org/compliance/gdpr/information_sharing_and_cooperation_gdpr.html

Morris, R. (n.d.). A history of cyber insurance. Retrieved from Marsh Commercial: https://www.marshcommercial.co.uk/articles/history-of-cyber-insurance/

n1nj4sec. (2019). Pupy. Retrieved from GItHub: https://github.com/n1nj4sec/pupy

n1nj4sec. (2021). n1nj4sec / pupy. Retrieved from GitHub: https://github.com/n1nj4sec/pupy

Nakashima, E. (2018, January 12). Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes. Retrieved from Washington Post: https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html

nettitude. (2021). PoshC2. Retrieved from GitHub: https://github.com/Nettitude/PoshC2

New York Department of Financial Services. (2021, February 4). Insurance Circular Letter No. 2 (2021) Cyber Insurance Risk Framework. Retrieved from New York Department of Financial Services: https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02

Rand, J. M. (n.d.). MONDELEZ-INTERNATIONAL-INC-Plaintiff-v-ZURICH-AMERICAN-INSURANCE-COMPANY-Defenda.pdf. Retrieved from Cyberinsurance Law Blog: https://www.databreachninja.com/wp-content/uploads/sites/63/2019/01/MONDELEZ-INTERNATIONAL-INC-Plaintiff-v-ZURICH-AMERICAN-INSURANCE-COMPANY-Defenda.pdf

Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021. (2021). Retrieved from U.S. Treasury Financial Crimes Enforcement Network: https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf

Rapid7. (2021). metasploit. Retrieved from Rapid7 Metasploit: https://www.metasploit.com/

Rapid7. (2021). Meterpreter. Retrieved from GitHub: https://github.com/rapid7/metasploit-framework/wiki/Meterpreter

RIces. (2021). Phishious. Retrieved from GItHub: https://github.com/Rices/Phishious

rsmudge. (2021). armitage. Retrieved from GitHub: https://github.com/rsmudge/armitage

Scism, L. (2021, October 8). Allstate Wants to Track Your Driving to Determine Your Car Insurance Rate. Retrieved from The Wall Street Journal: https://www.wsj.com/articles/allstate-wants-to-track-your-driving-to-determine-your-car-insurance-rate-11633685400

Scism, L. (2021, November 3). Insure-Tech Firm Lemondade to Offer Car Insurance. Retrieved from Wall Street Journal: https://www.wsj.com/articles/insure-tech-firm-lemonade-to-offer-car-insurance-11635935400

Sharma, A. (2021, October 25). Popular npm Project Used by Millions Hijacked in Supply-Chain Attack. Retrieved from Sonatype: https://blog.sonatype.com/npm-project-used-by-millions-hijacked-in-supply-chain-attack

Social Security Actuarial Life Table. (n.d.). Retrieved from ssa.gov: https://www.ssa.gov/oact/STATS/table4c6.html

SpiderLabs. (2021). Responder. Retrieved from GitHub: https://github.com/lgandx/Responder

Systems, H. (2021). Cobalt Strike. Retrieved from Cobalt Strike: https://www.cobaltstrike.com/

The Recorded Future Platform. (n.d.). Retrieved from Recorded Future: https://www.recordedfuture.com/platform/

Types of Personal Insurance Coverage. (n.d.). Retrieved from trisure.com: https://trisure.com/personal-insurance/types-of-coverage/

Voreacos, D., Chiglinsky, K., & Griffin, R. (2019, December 02). Merck Cyberattack's $1.3 Billion Question: Was It an Act of War? Retrieved from Bloomberg: https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war

Zip Codes Covered by Mandatory One Year Moratorium on Non-Renewals. (n.d.). Retrieved from California Department of Insurance: https://www.insurance.ca.gov/01-consumers/140-catastrophes/wildfirenonrenewalinfo.cfm

Levi Gundert is the SVP of Global Intelligence at Recorded Future.
He lives in Southern California.