Cymulate
Extended Security Posture Management

# Are Cyber-Insurance Models Broken?

Bridging the gap between cyber-insurance models and reality


Cymulate

# Table of Contents

# 01 Abstract

The evolution of cyber-crimes in the last decade, and particularly since the combination of commoditization of advanced hacking tools, the facilitation of ransomware through hard to trace crypto-currency payments, and the abrupt migration to remote working due to the pandemic, points unequivocally towards an increase in cyber-risks for the foreseeable future, from ransomware and other malware drops to data exfiltration and spying activity.
As a result, the cyber-insurance market is seeing claims value reaching up to three times the initial claim amount while underwriting a cyber-insurance policy is becoming increasingly complex due to the advanced technological knowledge required, especially with an endemic shortage of skilled cyber-security professionals.

In parallel, industries across all verticals as well as governmental institutions and NGOs are increasingly looking to purchase cyber-insurance, a situation that is likely to continue for the foreseeable future and might even escalate if regulators require certain bodies to acquire cyber-insurance in order to be compliant.

With the pace of change accelerating, cyber-insurance providers need to adapt fast and adjust today's cyber-insurance underwriting process to the reality of tomorrow's cyber-crime landscape.
After a brief overview of the state of cyber-insurance today, this paper examines the technological side of underwriting cyber-insurance policies.
It delves into the clear link between the need for technological acumen in evaluating insured parties' security posture and its fluctuations, and the structural flaws in most risk assessment methods before introducing and detailing how emerging technological options can facilitate the risk-evaluation part cyber-insurance underwriting without requiring advanced technical knowledge from the underwriter.

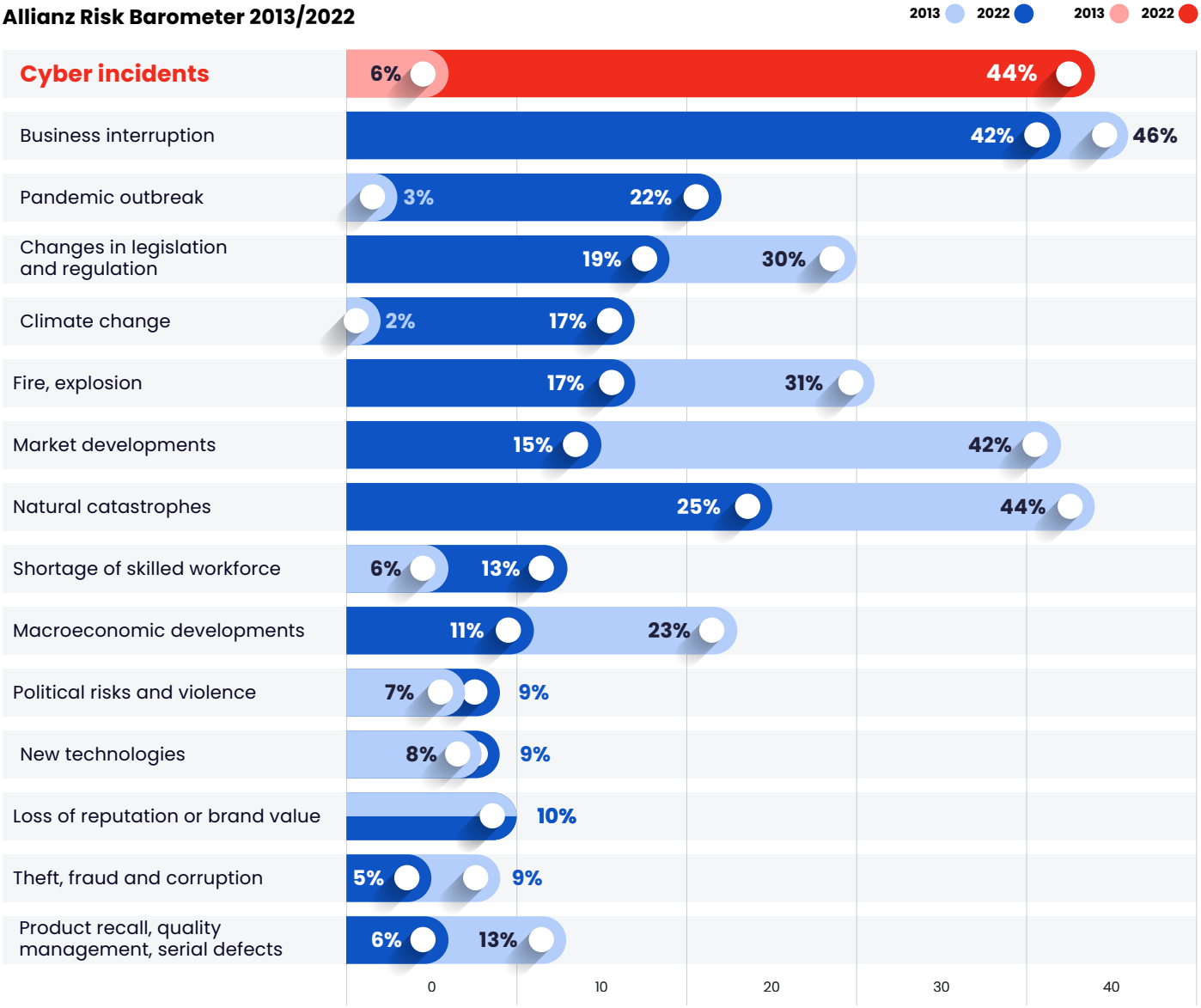
# 02 | The Cyber-Insurance Market Today

In line with Gallagher 2020 predictions that, given the increasingly complex scope of cyber risk and scale of expected claims, significant rate increases for cyber insurance purchasers at renewal is a fair and realistic expectation, cyber-insurance claims paid under cyber insurance policies are significantly up these last two years according to Marsh November 2021 report, The Changing Face of Cyber Claims.

The annual World Economic Forum Global Risk Report 2022 ranks "cybersecurity failure" as one of the top-10 risks that have worsened most since the start of the COVID-19 crisis and reports that 85% of their Cybersecurity Leadership Community stressed that ransomware is becoming a major concern for public safety. Regionally, APAC, Europe, and several highly digitalized economies – such as Denmark, Israel, Japan, Singapore, or the United Arab Emirates - rank "cybersecurity failure" within the top five risks, while Australia, Great Britain, Ireland, and New Zealand identify it at the highest risk of all.

Most strikingly, the yearly Allianz Risk Barometer of the most important business risks shows cyber incidents jump from a third-to-last position in 2013 with a 6% score to the first position with a 44% score in 2022, overcoming Business Interruption the facto that had comfortably been leading since 2013.

**Allianz Risk Barometer 2013/2022**



This acute preoccupation with cyber incidents is more than justified and, for example, the estimated 2021 225% increases in ransomware-related losses compared to 2020, losses estimated at $20 billion Looking only at ransomware, the pace of attacks has increased from one attack every 40 sec in 2019 to one attack every 11 seconds in 2021.
The cost of ransomware is not limited to the ransom amount and the costs linked to business interruption, but also covers loss of business, C-Level talent loss, employees layoff, reputational damage, further extortion using exfiltrated data as blackmail, reputational damage due to the publication and/or sale of the exfiltrated data, legal fees and the list goes on. The rise in ransomware attacks' number and seriousness combined with its designation as a national risk by President Biden and culminated in widely publicized governmental actions such as the Counter-Ransomware Initiative were instrumental in pushing the awareness of the risks associated with cyber incidents in general.
With the risk perception steadily rising, it is not surprising that the cyber-insurance industry experienced a 33.5% growth in 2020 alone and is forecasted to reach US$ 20.56 billion by 2025.

**Global Cyber Insurance Market ($bn), 2015-2025f**


Source: GlobalData, Insurance Intelligence Center

**The extent of damages to cover:**

- Ransom payment
- Business operation interruption
- Data recovery
- Reputational damages
- Digital infrastructure damages
- Fines for non-compliance
- Damages to third parties
- Other

**The inability to quantify the insured security posture**

Based on hard data stems from the observability gap explored more in-depth below.

The fast-evolving nature of the cyber-insurance field led major insurers to band together and create Cyber Acu View, a think tank dedicated to the cyber insurance segment.

# 03 | Why is re-inventing the process of cyber-insurance underwriting urgent?

Cyber-insurance underwriting needs to evolve apace with the rapidly evolving cyber landscape. At its source, the evolution of cyber-risk stems from four separate factors:

**The surge of cyber-criminal activity**
Cyber-criminals activity led to a 125% increase in cyber-intrusions in the first half of 2021, compared with the same period in 2020, 62% increase in ransomware incidents through the first six months of 2021 in the US, which followed a 20% increase in the number of incidents in 2020, and a 225% increase in ransom demands.
The Increased attack-sophistication and the ballooning number of attacks targeting all industry sectors are likely to get worse before they get better. Curbing the economics of cyber-crime to the point where it significantly impacts its prevalence requires international cooperation and widespread incorporation of increased cyber-defense.
As the elements to evaluate a timeline for achieving impactful results include global cooperation and drastically increased digital literacy for internet users, curbing cyber-crime is unlikely to happen soon. From the perspective of underwriting cyber-insurance, this side of the equation is entirely external to the insured party, and its evaluation relies on macro data. It will not be further analyzed in this paper.

**The constantly evolving nature of the digital environment**
Resulting from the wide-ranging adoption of agile development borne out of the business necessity of continually updating and deploying upgrades and new features, the massive adoption of the cloud, and the ever-more interconnected nature of the digital world with the resulting ever-present risk of supply-chain attacks.

**The insured party cyber-risk profile**
Until the advent of cloud computing, which began to take off in 2006 and is now fast becoming the default option, cyber-security architecture typically relied on a closed network. This means evaluating a cyber-risk profile would consist in checking if the perimeter was secure.
The new cloud-based or hybrid architecture renders the entire perimeter concept obsolete and ushered in the zero-trust concept based on a combination of segmentation and least privilege access approach guiding the configuration of security control policies. In addition, an ever-growing array of detect-and-response technological solutions too often devolves into an un-understandable tool sprawl, turning assessing the insured profile into a highly technical process.
With the endemic cybersecurity skills gap, finding an underwriter with the necessary and up-to-date technological knowledge is a challenge that can best be solved with easy-to-use and continuously updated evaluation tools.
Repurposing an Extended Security Posture Management solution for cyber-insurance underwriting purposes is an immediately available option.

**The growing extent of damages to cover:**
In addition to the classic Business Interruption, Data Recovery and Infrastructure damages, insured parties are now seeking to get coverage for emerging risks such as

- **Cyber-Extortion Costs**: as a direct consequence of the surge in ransomware, and despite the evolving legal status of paying the ransom, cyber-extortion coverage typically covers monies to pay ransom demands, the cost of hiring experts to negotiate with hackers and the cost of computer forensics experts.
- **Reputational Risks**: The negative coverage following a cyber breach has cascading effects ranging from stock price dips to loss of customer and brand damage.
- **Fines for non-compliance:** Regulatory bodies' requirements for data protection are adapting to the evolving technology and getting consistently more stringent. At the same time, as more and more regulatory authorities are issuing fines for non-compliance, a single infraction can lead to multiple fines.

In addition, the technology sector's hunger for Third-Party Cyber Liability covering damages transitively derived from digital products is growing, and the increased connectivity of the Internet of Things (IoT) and Operating Technology (OT) will probably lead to an entirely new and fast-growing series of emerging risks.

## The technological factor in cyber-insurance underwriting

According to AGCS 2022 Allianz Risk Barometer report, today's focus of underwriters is to place increased scrutiny on the cyber security controls employed by organizations to guide their pricing decision. This aligns with the findings of the June 2021 UK Royal United Services Institute for Defence and Security Studies paper Cyber Insurance and the Cyber Security Challenge that recommends assessing risk profiles and security practices and linking risk profiles and best practices to financial incentives.

Today, the underwriter typically relies on three main angles of inquiry:

- **Adherence to best practices**
  The recommended tools to assess an organization cyber security posture are typically based on adherence to Best Practices by Standard Institutes such as the NIST (National Institute of Standards and Technology) Cybersecurity Framework, the CIS (Center for Internet Security) Critical Security Controls, or OWASP (Open Web Application Security Project) Security Knowledge Framework.

- **Penetration testing**
  Now mandated by a growing number of regulatory bodies, a yearly penetration test is becoming a minimum requirement to be compliant and, despite its inherent limitations covered below, access to the penetration test report can provide useful information to the underwriter.

- **Cyber-resilience assessment**
  Emerging additional evaluation elements are looking at the resilience factor, meant to evaluate the potential extent of a successful breach, the time needed to mitigate it and to resume unimpeded operations if the breach led to business slowdown or interruption.
  The Cybersecurity & Infrastructure Security Agency (CISA) provides self-assessment and guided resources to assess cyber-resilience.
  The frequency and scope of Tabletop Exercises (TTE) or other breach simulation exercises performed by the organization can also be factored in to evaluate its cyber-resilience.

Aside from the technological know-how needed to evaluate how closely the prospective insured party is following these best practices and the time-limited value of a penetration test, any result born of an evaluation performed at a specific time has a shelf-lifetime value shorter than even a yearlong policy, as delineated in the section below, and should be shored up by other elements, such as those suggested below.

## The issues with current methods of assessing risk profiles and security practices

In the absence of a unified yardstick to evaluate cyber-resilience, underwriting cyber-insurance is condemned to include considerable reliance on the underwriter's ability to guestimate accurately. There are technological reasons behind the inherent lack of precision of the evaluating resources listed above, and the lack of access to a tool defining accepted standards leads to widely uneven evaluations.

### The issues with evaluating security posture based on best practices

There are quite a few issues with blind reliance on best practices for security posture evaluation. Best practices are, by definition, defined to suit everyone. Yet, as organizations are as varied as humans, their value needs to be adjusted to match the organizations' specific case:

- Not all best practices are relevant to every organization. Some might be privileged over others for perfectly justifiable reasons, while others might be neglected only to streamline the production process. The high level of technological acumen required from an underwriter to accurately assess the technological logic behind some misalignment with best practices is too high to be practicable.

- Even following all the best practices does not provide hermetic security. In its Cybersecurity Quarterly Winter 2021 whitepaper, the CIS states that following its best practices protects against 86% of MITRE ATT&CK sub-techniques (MITRE ATT&CK is an open-source framework opened by the US Department of Defense listing all known cyber-attacks tactics, techniques, and procedures). Or, in other words, perfect abidance to all best practices still leaves the organization wide open to 14% of known attacks.

- Some best practices, such as comprehensive patching, are unattainable. Though applying patches as soon as they appear is undoubtedly an efficient way to limit exposure, the combination of the sheer number of vulnerabilities to patch and the technical complexities involved in patching without breaking things. Even limiting patching to vulnerabilities with a CVSS score above 9 is unrealistic. Out of the 20184 new vulnerabilities uncovered in 2021, 1165 scored above 9.

- Applying best practice continuously is not evaluated accurately through a one-time, or even yearly, evaluation.

**The issues with evaluating security posture through penetration testing**

The only guaranteed result of running a penetration test is that it protects from non-compliance fines related to the obligation of running a yearly penetration test. All the rest is fraught with issues.

- Though penetration testing used to be the golden standard in security posture validation, the technology has evolved, and the results of a penetration test are highly dependent on the tester's ability and tooling.
  In the age of ML/AI-assisted hacking tools available as SaaS to cyber-criminals, validating an organization security posture requires advanced offensive testing, at a minimum, a red teaming exercise.

- Even with an optimal penetration test identifying every single security gap, a single test performed once a year provides a snapshot of the organization at a point in time. With agile development, based on pushing new deployment fast and often, the test has a short time relevancy as it is only valid until the next deployment that might introduce new security gaps or close some.

**The issues with evaluating security posture through cyber-resilience**

Undoubtedly a step in the right direction, privileging cyber-resiliency over the classic focus on data-protection characteristic of classic cyber-security might lead to a sorely needed change leading to a multi-dimensional approach that dynamically responds to threats while keeping business goals intact. However, the comprehensive cyber-resiliency evaluation tools are still barely emerging, and the manual approaches available as guidance are complex and still at a nascent stage. Though warmly encouraged by the World Economic Forum, the creation of a Common Cyber Resiliency framework is still in the future. The closest existing cyber-resiliency tool is an Extended Security Posture Management (XSPM) platform, and this tool could be adapted to serve as the base for a Common Cyber-Resiliency Framework and standardize the security posture scoring system.

> *"Insurers' inability to observe an organization's internal protection efforts has posed significant challenges to cyber insurance. The observability gap is an even bigger challenge for claims and the near impossibility to correlate losses to a specific cyber incident. There is a dire need for adequate risk observability."*
>
> Scott Sayce, Global Head of Cyber at AGCS

# 04 The Future of Cyber-Insurance Continuous Dynamic Underwriting Evaluation

For cyber-insurance to become a mainstay of the digital economy as a widely available, widely affordable, consistently priced product:

- Cyber-risks must be mitigated through enhanced cybersecurity
- Cyber-risk exposure must be consistently measurable
- Cyber-risk must be continuously validated
- Consistent benchmarks must be widely accepted

The first three points can be achieved through technological progress and are already available with the emerging Extended Security Posture Management (XSPM) basket of technologies and could easily be integrating with cyber-risk evaluation for insurance purposes to:

**01**

**Understand the applicant's security posture -** Assessing the insured party security posture from an offensive perspective by using a comprehensive array of agent-based and agentless production-safe attacks provides an in-depth overview of the actual security posture and enables quantifying the risk exposure. An XSPM platform can be used by the insurer to evaluate the insured party's exposure even if the insured party is not consistently using an XSPM approach.

**02**

**Improve ROI with adequate premiums and coverage -** A quantified security posture assessment provides a security score defined at global and granular levels and immensely facilitates correlating premium and coverage with actual, measurable risk levels.

**03**

**Lower the risk exposure AT the covered entities -** Insured parties consistently using the XSPM approach see their risk exposure diminish over time and avoid unnoticed security drift.

**04**

**Continuous audits of covered entities' security-** By design, an XSPM approach includes a continuous security posture audit, and provides updated security scores that could be used to condition coverage to a bracket of security scores. Insured parties using an XSPM platform consistently avoid the risk of hidden security drift and increased exposure.

**05**

**Minimize Impact of Potential Cyberattacks** – An XSPM approach includes actionable mitigation recommendations designed to optimize the mitigation process and reduce risks of escalation and lateral movement. The waterfall damages at an insured party consistently using an XSPM platform are considerably reduced, minimizing the amount to be paid for damages.

The creation of consistent benchmarks will require the collaboration of the various cyber-insurance actors and could be based on security scores created by XSPM platforms.

## The XSPM Factor

Extended Security Posture Management (XSPM) is a comprehensive suite of continuous security validation tools under a single platform that provides a quantified evaluation of an organization security posture and monitors security drift. Through extensive arrays of production-safe attacks mimicking both MITRE ATT&CK TTPs and emerging threats scenarios, it identifies security gaps exploitable by cyber-attackers and provides actionable mitigation recommendations to close those gaps.

**Attack Surface Management (ASM)**
ASM is a technology that scours the internet to identify all exposed assets related to the organization. Once all these assets are cataloged, they can be monitored.

**Breach and Attack Simulation (BAS)**
BAS technology simulates a large array of attacks to test the resilience of an organization's digital infrastructure resiliency to attack.
BAS works on several attack vectors, such as email security, web gateway, web application firewall, lateral movement, and data exfiltration.
Each of these vectors is scored, enabling granular visibility and improvement of each vector score.
Full BAS solutions also provide a full kill chain option that measures the ability of an attacker to progress unimpeded within the infrastructure regardless of the vector. BAS provides actionable remediation recommendations for each identified security gap.

**Immediate Threat Intelligence (ITI)**
ITI provides organizations with testing and remediation tools for threats as they emerge, enabling them to immediately evaluate the organization's risk exposure to emerging threats and preemptively block emerging Indicators of Compromise (IoCs) when necessary.
his effectively means that it drastically limits exposure to even brand-new types of attacks.

**Continuous Automated Red Teaming (CART)**
CART is an automated version of penetration testing that utilizes hacking technologies and tests the organization's permeability to breaches from the moment the attacker breaches in. Depending on the success of the simulated attacker, a security score is attributed, and actionable remediation recommendations for each identified security gap are provided.

**Attack-Based Vulnerability Management (ASBM)**
ASBM is the most advanced Vulnerability Prioritization Technology (VPT) available.
Its use is contingent on using offensive testing methods such as BAS, ITI, and CART, and prioritizing the vulnerability patching schedule based on the risk they pose to the organization's digital infrastructure specifically as opposed to VPTs (Vulnerability Prioritization Technology) based on best practices.

An XSPM platform is conceived to run continuously, so security drift is constantly monitored and immediately reflect both modifications in the digital infrastructure following a new deployment and exposure to emerging threats

**Phishing Awareness**
Humans remain a critical risk factor, and the main way cyber-attackers try to "breach" humans is through phishing. A phishing awareness module launches fake phishing campaigns to evaluate:

- The likelihood that an employee will click on a phishing email
- The ability of email security solution configuration to stop the progression of a production-safe attack included in the email

The resulting report enables organizations to identify:

- Weak links in their ranks and retrain them for enhanced awareness
- Gaps in the email security configuration that can then be fixed.

A phishing awareness score is also attributed to the organization. The XSPM platform then correlates all these scores to quantify the overall security posture of the organization.

## Underwriting Cyber-Insurance with XSPM

**Even in the absence of globally accepted benchmarks, from a cyber-insurance underwriter perspective, using XSPM as a cyber-insurance underwriting evaluation tool could already solve a number of policy creation pre-binding phase issues:**

- Assessments performed with XSPM eschew the drawbacks of relying on reliance on best practices – XSPM comprehensive assessments by nature measure the security posture of the organization based on its actual resilience to attacks instead of a theoretical projection of the security obtained through abidance to best practices.
- The risk score is globally and granularly quantified – access to off-the-shelf quantified risk score eliminates the need for advanced technological knowledge for the underwriter.
  Access to a granular scoring of the security scores per vector could enable underwriters to fine-tune premium evaluation based on the insured activity and the activity's relation to each vector.
- Running a full XSPM assessment requires very little technological prior knowledge and can be learned in a one- or two-days training session.

In addition, it could be adapted to creatively redefine the post-binding phase or create a cyber version of the seatbelt defense:

- The continuous nature of XSPM could be used to define post-binding phases of a policy by requiring periodic re-evaluation and/or reporting on the global security posture or on a sub-set of scores calibrated to match the insured party specificities as XSPM has the ability to verify if the customer's security posture changed over a period of time during the coverage period.
- Requirements such as correcting variance from agreed-upon baselines within a reasonable time frame could be imposed on the insured. The policy could include an obligation to share the automated generated report after each assessment and link the relative amount of payment payable in case of breach to documented abidance to baseline variance. Non-compliance could affect the degree of coverage and/or required premiums.

All of the above can already be used in cyber insurance underwriting with XSPM.
In the future, one might imagine integrating XSPM scoring with risk evaluation modeling and automating a part of the underwriting process to accelerate it and enable scaling up.

> *By sharing information and developing a common foundation in which to underwrite constantly evolving cyber risks, the industry will be better equipped to provide the proper coverage and solutions to protect organizations from cyber-related exposures.*
>
> Russ Cohen, Director of Cyber/Privacy Services at Chubb

# 05 Sources

Some of the sources are hyperlinked within the text and some are not as it would hamper readability. All the documents referred to below have been used as information sources to create this White Paper.


- Accenture – 2021 - Risk mitigation for cyber insurance: Digital tools, twins and ecosystems - https://insuranceblog.accenture.com/risk-mitigation-cyber-insurance-digital-tools-twins-ecosystems
- Allianz – 2022 – Allianz Risk Barometer - https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html
- Bank of England Prudential Regulation Authority – 2021 – Insurance Stress Test 2022 (IST 20222) – https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2021/august/insurance-stress-test-2022.pdf
- Business Insurance – 2021 - Cyber insurance premiums soar: RPS - https://www.businessinsurance.com/article/20211005/NEWS06/912345022/Cyber-insurance-premiums-soar-RPS,-Risk-Placement-Services-Inc
- CIS Security – 2021 – Cybersecurity Quarterly Winter – p. 18 - https://www.cisecurity.org/white-papers/cybersecurity-quarterly-winter-2021/
- CIS Security – 2021 – CIS Controls List - https://www.cisecurity.org/controls/cis-controls-list/
- CISOMAG – 2021 - Hardening Cyber Insurance Market Makes Cybersecurity More than a Tech Problem - https://cisomag.eccouncil.org/hardening-cyber-insurance-market-makes-ctbersecurity-more-than-a-tech-problem/
- CISOMAG – 2021 - Demystifying Cyber Insurance to Enable Adoption - https://cisomag.eccouncil.org/demystifying-cyber-insurance/
- Clyde & CO – 2021 - US insureds face stricter cyber insurance underwriting requirements and greater enforcement of privacy laws - https://www.clydeco.com/en/insights/2021/12/us-insureds-face-stricter-cyber-and-privacy-laws
- CPO Magazine – 2022 - Putting Skin in the Cyber Insurance Game - https://www.cpomagazine.com/cyber-security/putting-skin-in-the-cyber-insurance-game/
- CVE Details- https://www.cvedetails.com/cvss-score-charts.php?fromform=1&vendor_id=&product_id =&startdate=2021-01-01&enddate=2022-01-01
- CyberCrime Magazine – 2021 - Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031 - https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/
- Cybersecurity Cooperative Research Centre – 2021 - Underwritten
- or Oversold? - https://cybersecuritycrc.org.au/sites/default/files/2021-10/Underwritten%20or%20oversold%20%20-%20DV.pdf
- Cybereason – 2021 - Report: Ransomware Attacks and the True Cost to Business - https://www.cybereason.com/blog/report-ransomware-attacks-and-the-true-cost-to-business
- CyberTechInsider – 2022 - The End of the Golden Age of Ransomware? - https://www.cybertech-insider.com/post/the-end-of-the-golden-age-of-ransomware
- Dark Reading – 2022 - Breach Response Shift: More Lawyers, Less Cyber-Insurance Coverage - https://www.darkreading.com/attacks-breaches/changes-to-breach-response-more-lawyers-less-cyber-coverage
- Deloitte – Global - A framework for quantifying cyber risk: Pipedream or possible? - https://www2.deloitte.com/global/en/pages/risk/articles/a-framework-for-quantifying-cyber-risk-pipedream-or-possible.html
- Deloitte – UK - Cyber insurance underwriting - Helping boards create supervisory confidence - https://www2.deloitte.com/uk/en/pages/risk/articles/cyber-insurance-helping-boards-create-supervisory-confidence.html
- Deloitte – global - Cyber risk and regulation in Europe - https://www2.deloitte.com/global/en/pages/risk/cyber-strategic-risk/articles/gx-cyber-risk-and-regulation-in-europe.html
- Deloitte – UK - Cyber insurance underwriting - Helping boards create supervisory confidence - https://www2.deloitte.com/uk/en/pages/risk/articles/cyber-insurance-helping-boards-create-supervisory-confidence.html
- Deloitte – UK – 2021 - Cyber insurance underwriting Part I: Back on the supervisory agenda - https://ukfinancialservicesinsights.deloitte.com/post/102h8wy/cyber-insurance-underwriting-part-i-back-on-the-supervisory-agenda
- Deloitte – UK – 2021 - Cyber insurance underwriting Part II: Silent cyber risk still biggest concern - https://ukfinancialservicesinsights.deloitte.com/post/102h9d1/cyber-insurance-underwriting-part-ii-silent-cyber-risk-still-biggest-concern
- Forrester – 2021 - The Cyber Insurance Roller Coaster: As Demand Speeds Up, Some Insurers Disembark - https://www.forrester.com/blogs/the-cyber-insurance-roller-coaster-as-demand-speeds-up-some-insurers-disembark/
- NIST – Cybersecurity Framework - https://www.nist.gov/cyberframework
- Financier Worldwide – 2015 - A new approach to risk assessment for cyber insurance - https://www.financierworldwide.com/a-new-approach-to-risk-assessment-for-cyber-insurance#.Ye0ECf7P1PY
- Foreign Affairs – 2022 - How to Cyberproof the Private Sector - https://www.foreignaffairs.com/articles/north-america/2022-01-13/how-cyberproof-private-sector
- Gallagher- 2021- International Perspectives Report – Downloadable from https://www.ajg.com/be/international-perspectives-report/
- GlobalData – 2021 - Cyber insurance industry to exceed $20bn by 2025, says GlobalData - https://www.globaldata.com/cyber-insurance-industry-exceed-20bn-2025-says-globaldata/
- Insurance Journal – 2021 - Biz Interruption, Recovery Costs Drive Financial Losses from Cyber Attacks: Report - https://www.insurancejournal.com/news/international/2021/10/14/637049.htm

- International Association of Insurance Supervisors (IAIS)- 2020 - Cyber Risk Underwriting Identified Challenges and Supervisory Considerations for Sustainable Market Development - Downloadable from https://www.iaisweb.org/page/supervisory-material/other-supervisory-papers-and-reports/file/94255/cyber-risk-underwriting-identified-challenges-and-supervisory-considerations-for-sustainable-market-development
- Harvard Business Review – 2021 - Cybersecurity Insurance Has a Big Problem - https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem
  Hiscox – 2021 - Hiscox Cyber Readiness Report - https://www.hiscox.co.uk/cyberreadiness
- JDSUPRA – 2022 - Does Your Cyber Insurance Policy Look More Like Health Insurance? - https://www.jdsupra.com/legalnews/does-your-cyber-insurance-policy-look-6154384/
- Lawfare – 2021 - Ransomware Payments and the Law - https://www.lawfareblog.com/ransomware-payments-and-law
- Marsh – 2021 – Global Insurance Market Index - https://www.marsh.com/il/en/services/international-placement-services/insights/global_insurance_market_index.html
- Marsh – 2021 – The Changing Face of Cyber Claims - https://www.marsh.com/il/en/services/cyber-risk/insights/the-changing-face-of-cyber-claims-2021.html
- Marsh Mc Lennan – 2022 - Global Risk Report - https://www.marshmclennan.com/insights/publications/2022/january/global-risks-report.html
- National Association of Insurance Commissioners (NAIC) – 2021 - NAIC Report Show 2020 Premiums Grew 29.1% as Cyberthreats Rise - https://content.naic.org/article/naic_report_show_2020_premiums_grew_291_cyberthreats_rise.htm
- Reinsurance News – 2022 - Cyber requires significant investment in underwriting: Beazley - https://www.reinsurancene.ws/cyber-requires-significant-investment-in-underwriting-beazley/
- Reuters – 2021 - Insurers run from ransomware cover as losses mount - https://www.reuters.com/markets/europe/insurers-run-ransomware-cover-losses-mount-2021-11-19/
- Royal United Services Institute for Defence and Security Studies (RUSI) – 2021 - The UK Government's New Cyber Strategy: A Whole of Society Response - https://rusi.org/explore-our-research/publications/commentary/uk-governments-new-cyber-strategy-whole-society-response
- Royal United Services Institute for Defence and Security Studies (RUSI) – 2021 - Cyber Insurance and the Cyber Security Challenge - https://static.rusi.org/247-op-cyber-insurance-fwv.pdf
- Security Magazine – 2021 - The rising tide of cyber insurance premiums in the age of ransomware - https://www.securitymagazine.com/articles/96549-the-rising-tide-of-cyber-insurance-premiums-in-the-age-of-ransomware
- Security Magazine – 2021- How cyber underwriters can better respond to the current cyber pandemic - https://www.securitymagazine.com/articles/96779-how-cyber-underwriters-can-better-respond-to-the-current-cyber-pandemic
- Society of Actuaries – 2017 - Cybersecurity Insurance: Modeling and Pricing - https://www.soa.org/globalassets/assets/files/research/projects/cybersecurity-insurance-report.pdf
- Sophos News – 2021 - What's next for cyber insurance? - https://news.sophos.com/en-us/2021/11/24/whats-next-for-cyber-insurance/
- TechRepublic – 2021 - The cybersecurity skills gap persists for the fifth year running - https://www.techrepublic.com/article/the-cybersecurity-skills-gap-persists-for-the-fifth-year-running/
- TechTarget – 2021 - Why patching vulnerabilities is still a problem, and how to fix it - https://www.techtarget.com/searchsecurity/news/252503950/Why-patching-vulnerabilities-is-still-a-problem-and-how-to-fix-it
- Tech Target – 2021 – Cyber Insurance Premium Costs Skyrocket as Attacks Surge - https://www.techtarget.com/searchsecurity/news/252507932/Cyber-insurance-premiums-costs-skyrocket-as-attacks-surge
- The White House – 2021 - Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021 -https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/
- Trend Micro – 2021 - Cybersecurity Tool Sprawl Drives Plans to Outsource Detection and Response - https://newsroom.trendmicro.com/2021-10-12-Cybersecurity-Tool-Sprawl-Drives-Plans-to-Outsource-Detection-and-Response
- VOUCH Resources – 2022 - Cyber Insurance for Startups: Top Concerns and Insights - https://www.vouch.us/knowledge/cyber-insurance-for-startups-top-concerns-and-insights
- World Economic Forum – 2021 - Cyber security is no longer enough: businesses need cyber resilience -


## About Cymulate

With a Research Lab that keeps abreast of the very latest threats, Cymulate proactively challenges security posture end to end, automatically and continuously, allowing hyper-connected organizations in all maturity levels to avert damage and stay safe. Founded by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is trusted by hundreds of companies worldwide, from small businesses to large enterprises, including leading banks and financial services. They share our vision to be the gold standard for security professionals and leaders to manage, know and control their Cybersecurity Posture. Today it's simple for anyone to protect their company with the highest levels of security. Because the simpler cybersecurity is, the more secure your company-and every company-will be.




Headquarters: Maze St 3, Tel Aviv 6578931, Israel | +972 3 9030732 | info@cymulate.com | US Office: +1 212 6522632