EBOOK

How Continuous Underwriting is Transforming Cyber Insurance

SecurityScorecard.com
info@securityscorecard.com

©2022 SecurityScorecard Inc.

SecurityScorecard HQ
Tower 49
12 E 49th St
Suite 15-001
New York, NY 10017
1.800.682.1707

SecurityScorecard

EXECUTIVE SUMMARY

While **cyber insurance has never been more desperately required by businesses of all sizes**, insurance carriers often struggle to appropriately evaluate their risk. As a result, insurers are significantly increasing their premiums, reducing coverage, or exiting the cyber insurance market completely – frustrating customers in the process.

To better control their exposure to the unique risks posed by cyber crime, insurers must leverage a new process to remain agile and responsive. We call that process continuous underwriting.

In this ebook, we'll help you understand how a continuous underwriting approach works, challenges to watch for, and why security ratings are an essential tool for enabling a continuous underwriting process.

UNDERSTANDING THE
CYBER INSURANCE LANDSCAPE

In just a few years, cyber insurance evolved from a little-considered business insurance add-on to a major policy in its own right. According to the U.S. Government Accountability Office, the proportion of existing clients electing cyber insurance coverage nearly doubled from 26% in 2016 to 47% in 2020[1].

Just as with any other insurance product, cyber insurance protects against losses caused by an event covered in the policy – in this case, losses from a cyber security incident. However, unlike home, auto, business, or other insurance types, cyber insurance is a relatively new market, making it difficult to accurately assess an insured's true risk.

Over the last two years, this lack of transparency into risk – coupled with an increase in the digital transformation of business, the rise of ransomware as a service, and the increasing complexity of technology – left insurers dangerously exposed to a significant increase in volume and impact of ransomware attacks. Since the pandemic, there were was a 151% increase in ransomware attack volume,[2] leading to a 311% increase in total ransoms paid.[3] As a result, cyber insurers experienced a record loss ratio of 67% as they paid out higher-than-expected insurance claims.[4]

This caused some insurers to either flee the market or offer less coverage, with 70% of brokers reporting capacity reductions [5]. Those who stayed significantly increased their premiums, with reports of cyber insurance pricing skyrocketing on average by ~50%. [6] The bottom line: the cyber insurance market has significantly hardened and continues to face headwinds, making it unlikely the market will stabilize in the short- or medium-term.

[1] https://www.gao.gov/products/gao-21-477

[2] https://www.sonicwall.com/news/sonicwall-record-304-7-million-ransomware-attacks-eclipse-2020-global-total-in-just-6-months/

[3] https://blog.chainalysis.com/reports/ransomware-ecosystem-crypto-crime-2021

[4] https://www.reinsurancene.ws/cyber-industry-loss-ratio-at-record-high-67-in-2020-aon/

[5] https://www.itpro.com/security/cyber-security/360131/cyber-insurance-premiums-increased-by-a-third-in-the-last-12-months

[6] https://www.insidepandc.com/article/2876n3df4whrwnzumcni8/chubb-overhauls-cyber-appetite-with-smaller-lines-and-rate-demands

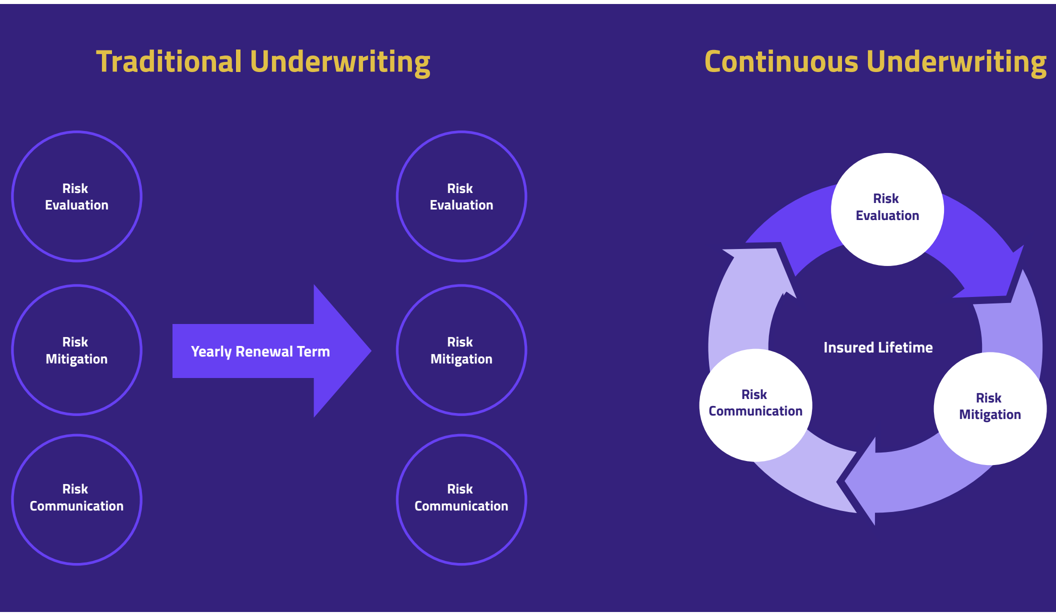
CONTINUOUS UNDERWRITING DEFINED

Why were carriers caught unprepared? The problem is that cyber insurers rely on the same point-in-time underwriting process they use to assess every other type of risk, despite the fact that cyber risk encompasses risk factors and assets that rarely remain static.

Consider property insurance: something like earthquake risk is well understood since it's governed by the unchanging laws of nature, with the outlook only changing in relatively minor ways as building technology improves. Single point-in-time risk underwriting works well for these types of risks.

Cyber risk is fundamentally different and the traditional underwriting approaches used by other insurance lines should not apply. In order to provide a cyber insurance product that can accurately protect both the policyholder and carrier, a new continuous underwriting approach is required.

Continuous underwriting is a process that enables insurers to constantly re-evaluate their risk so they have a better understanding of their liabilities. This allows insurers to align changes in their risk management activities with changes in their underlying risk. By keeping pace with changes in technology, trends, and risk, they can manage their portfolios accordingly to mitigate excess exposure.



Traditional Underwriting

Continuous Underwriting

WHY CONTINUOUS UNDERWRITING IS A CYBER INSURANCE REQUIREMENT

Continuous underwriting is critical to helping the insurance industry avoid another massive overcorrection like the one caused by the recent ransomware crime spree. Supply chain vulnerabilities, nation-state attacks, or something else could easily trigger the next wave of cyber incidents at any moment given that the speed and scale of cyber risk is unlike any other risk.

With continuous underwriting, insurance companies can keep a closer track of the cyber risk landscape and their policyholders to understand if and how new threats are increasing their cyber exposure. This keeps insurers and their policyholders engaged with each other throughout the year, not just at renewal.

In addition to helping carriers reduce exposure to larger-than-expected claims, it can provide policyholders with confidence that they are doing everything they can to prevent an attack, which can be far more costly in terms of reputation and business loss than any financial loss a claim might cover.

THE KEY ELEMENTS TO CONTINUOUS UNDERWRITING

At first glance, the process for continuous underwriting is the same as the standard insurance underwriting practices: you must still do your diligence to understand the risk posed by specific clients and your overall portfolio, and then adjust your premiums and coverages accordingly.

The key difference is that continuous underwriting allows carriers to gain a better understanding of their true risk on an ongoing basis while providing the information required to help policyholders reduce their risk. This process includes three elements:

- **Risk evaluation:**
  In this stage, the carrier will conduct a complete cyber insurance risk assessment to identify an organization's vulnerabilities. The insurer will often ask a policyholder to

outline its maturity across security governance, security architecture, specific cyber security tools, and their security risk management processes. The insurer may also use technology or third-party resources to identify vulnerabilities or issues. Based on findings from this assessment, an underwriter will evaluate the insurability of the organization and define the terms of the cyber insurance policy.

- **Risk mitigation:**
  In addition to accepting risk on behalf of the policyholder, a cyber insurance provider performs ongoing monitoring of the insured and helps provide risk prevention information, controls, and strategies so that clients can avoid an incident in the first place. Not only does this help protect the insurer from unnecessary loss, but it can help protect the policyholder from fines, legal fees, downtime, and other losses that cyber insurance may not cover.

- **Risk communication:**
  Risk mitigation is only as effective as an insurer's ability to convey actional information about a policyholder's risk and what they can do to minimize it. In this stage, the carrier will share their analysis of the policyholder's security posture, along with specific steps to take to better protect the organization. By creating deeper awareness about an organization's issues, the insurer can incentivize the right behaviors to reduce risk exposure.

OVERCOMING THE CHALLENGES OF CONTINUOUS UNDERWRITING

Let's face it: if it was simple, you'd likely already be using a continuous underwriting approach. Instead, you likely struggle to overcome one or more of the following challenges:

- **Monitoring the right data:**
  Even the average-sized organization can have hundreds of thousands of endpoints, credentials, internet-enabled devices, employees, servers, platforms, and other vectors for attack.

  As a result, an insurer can quickly become overwhelmed monitoring all this data, consolidating it, and analyzing it in time to make actionable, real-time recommendations.

- **Scaling outreach across the entire client portfolio:** Now multiply that challenge by the tens of thousands of cyber insurance policyholders an insurer might cover and you can see the problem.

  Every one of those organizations will have unique issues, but all can potentially be susceptible to the same major exploit. If you can't scale your ability to detect and communicate a strategy to protect each and every organization, it's almost as bad as not monitoring your risk at all. Even if you can communicate in time, you have to track and validate who is listening and the actions they take to make sure they maintain a strong cyber security posture.

- **Prioritizing risk mitigation strategies:** The reality is that every client will have far more vulnerabilities than they have people or resources to patch them.

  To help organizations reduce risk, you can't just send a list of every single issue you discovered; you must identify the 20% of the fixes that will achieve 80% of the impact. However, underwriters, brokers, or the policyholders themselves aren't necessarily cyber security experts, making it difficult to decide which issues are driving the most risk or what recommendations to make.

HOW SECURITY RATINGS ENABLE **CONTINUOUS UNDERWRITING**

In order to overcome the challenges of continuous underwriting, real-time, actionable data is a must. That's where security ratings come in.

A security ratings platform can analyze organizations, their third-party suppliers, and current threats to create an accurate picture of each insured's risk profile. By using objective data and predictive analytics to evaluate exposure, a cyber insurer can help customers identify, prioritize, and fix specific vulnerabilities so they can reduce the chances of an incident – thereby reducing the need to make a claim.

Insurers that incorporate a continuous underwriting approach can offer competitive premiums and coverage with the confidence that their portfolio is aligned with their overall risk tolerance. By using security ratings to power a continuous underwriting experience, carriers can achieve:

- **Improved cyber risk insight**
  A security ratings platform makes it easier to validate your policyholders' security postures with outside-in scans that accurately and non-intrusively identify what drives cyber risk for each customer. It can also help evaluate and score an organization's security posture over time so underwriters and brokers can understand if a customer is becoming more or less of a risk. Finally, underwriters can use security ratings to ensure that applicants fit within accepted risk tolerances for a healthy portfolio.

- **A more resilient business**
  A security ratings platform can alert you when it detects existing and new threats that might impact your customers so you can be protective instead of reactive. It will also score individual issues and vulnerabilities based on their business risk, helping you prioritize the security improvements that will have the most significant impact on a customer's overall score, leading to improved security postures.

- **More engaged customers**
  By helping policyholders improve their understanding and take decisive action, security ratings help you accomplish what you both want: to avoid a breach, ransomware attack, or other type of cyber security incident. A security ratings platform lets you offer self-monitoring for policyholders so they can become more engaged in their protection, while also helping you quickly communicate new threats. In addition, it can help validate responses so that underwriting becomes more of an ongoing collaboration that improves their business instead of feeling like a one-way interrogation.

ENABLE CONTINUOS UNDERWRITING **WITH SECURITYSCORECARD**

As the leading security ratings platform, SecurityScorecard is the only real-time data and analytics provider that can empower insurers to overcome the challenges of implementing continuous underwriting.

Our proven platform leverages automation to provide the most comprehensive and up-to-date view of global enterprises, with more than 12 million continuously rated companies available today. Thanks to our transparent data and analytical methods, insurers can go beyond general scores to understand the drivers of cyber risk in a way that is easy to understand. This helps insurers collaborate with policyholders to create data-driven risk reduction plans, all within one platform.

LEARN MORE ABOUT
SECURITYSCORECARD
FOR CYBER INSURERS

ABOUT
SECURITYSCORECARD

Funded by world-class investors including Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings with more than 12 + million companies continuously rated. Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, and cyber insurance underwriting. SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve and communicate cybersecurity risk to their boards, employees and vendors. Every organization has the universal right to their trusted and transparent Instant SecurityScorecard rating. For more information, visit **securityscorecard.com** or connect with us on **LinkedIn.**

When To receive an email with your company's current score, please visit **instant.securityscorecard.com.**

SecurityScorecard HQ
Tower 49
12 E 49th St
Suite 15-001
New York, NY 10017

www.securityscorecard.com
1 (800) 682-1707
info@securityscorecard.com
@security_score

SecurityScorecard