REDUCE CYBER RISK

with the predictive power of security ratings

SecurityScorecard | MarshMcLennan

Table of Contents

THE PROJECT TEAM

SecurityScorecard

Bob Sohval
Dmitry Lilko
Mike Woodward
Prashant Pai
Gian Calvesbert

Marsh McLennan Global Cyber Risk Analytics Center

Rush Kirubi
Carol Aplin
Scott Stransky
Wendy Hou-Neely

Nearly every organization today relies on digital connectivity to function, especially as consumer demands change and the number of smart devices grows. But this comes with inherent risk due to an expanding attack surface and the growing volume and frequency of ransomware attacks, phishing attempts, and data breaches. To protect themselves both legally and financially, many organizations understand the need for cyber insurance in the event of an incident. Yet a recent Forrester Research report found that only 55% of organizations in North America have cyber insurance, and of the companies that are insured, only 20% have more than $600,000 USD in coverage[1]. At a time when enterprises spend a mean of $2.4 million USD to find and recover from a breach, many organizations don't have the funds to cover their losses, let alone pay for downtime or legal fees[2].

Enterprises spend a mean of $2.4 million USD to find and recover from a breach

Cyber insurance is the fastest-growing sector of the world's insurance markets[3], and it's offered to companies of all sizes and in all industries. However, a recent increase in ransomware attacks has led to a sharp uptick in claims[4]. As a result, the cyber (re)insurance industry is looking for ways to help its customers increase their resilience, reduce their premiums, and improve their overall cyber hygiene. This requires a new methodology to measure risk in real time with greater accuracy. By working with cyber insurers to align on this risk, companies will be better able to get ahead of threats and obtain policies that meet their unique needs.

The **Marsh McLennan Global Cyber Risk Analytics Center** and **SecurityScorecard** have come together to study how cybersecurity ratings correlate with reduced cyber insurance risk. Marsh McLennan is charged with helping its clients understand and manage cybersecurity risk, which includes risk transfer options using cyber insurance. SecurityScorecard provides cybersecurity ratings and data, which offer measurable and actionable cyber risk insight.

[1] "The 2021 State of Enterprise Breaches," April 8, 2022
https://www.forrester.com/blogs/breaches-by-the-numbers-adapting-to-regional-challenges-is-imperative/

[2] "The 2021 State of Enterprise Breaches," April 8, 2022

[3] "25 Years: The Journey of Cyber Insurance," Insurance Journal, September 5, 2022
https://www.insurancejournal.com/magazines/mag-features/2022/09/05/683477.htm

[4] "Cyber Insurers Raise Rates Amid a Surge in Costly Hacks," Wall Street Journal, May 18, 2022
https://www.wsj.com/articles/cyber-insurers-raise-rates-amid-a-surge-in-costly-hacks-11652866200

A dynamic threat landscape requires **real-time risk assessment**

Investors in financial markets face a very similar problem to cyber insurers. They need to make investments, but have limited time and capacity to assess risk themselves. Assessing investment risk typically involves analysis of finances, the management team, the industry, and multiple other factors. To quickly and accurately model risk, investors rely on credit rating agencies that bundle risk factors into ratings. For investors, ratings solve the information asymmetry problem and essentially allow risk to be commodified.

Security ratings are an important factor used by the cyber (re)insurance industry in assessing cyber risk. Security ratings provide a function similar to credit ratings—namely packaging cyber risk into a handful of quantifiable factors. Cybersecurity ratings offer insurance companies the capability to accurately and rapidly provide quotes and manage their risk exposure, while offering customers the opportunity to manage and improve their security posture.

Cyber risk must be evaluated based on up-to-the-minute data; to reflect in near real-time, for instance, a new wave of ransomware attacks taking place. In all insurance markets, an underwriter would develop a form designed to help with a risk assessment. But because the nature of cyber risk is dynamic and ever-changing, it is difficult to use the 'form' methodology as the sole type of input for determining cyber insurance. For the last ten years, companies such as SecurityScorecard have offered cybersecurity ratings and scores that use continuous, external scanning to provide an outside-in view of risk in this constantly shifting landscape.

TO BUILD THESE SCORES, RATINGS COMPANIES DO THREE THINGS:

1. Build a map of digital assets (IPs and domains) owned or used by a company
2. Observe events and settings on these assets (CVEs, SPF settings, out-of-date browser detections, etc.)
3. Assign scores based on their observations and correlation to cyber incidents

[5] Cantor, Richard, and Frank Packer. "The credit rating industry." The Journal of Fixed Income 5, no. 3 (1995): 10-34

[6] Langohr, Herwig, and Patricia Langohr. "The rating agencies and their credit ratings: What they are, how they work, and why they are relevant." John Wiley & Sons, 2010.

Seven factors that can **predict a cyber breach**

In order to conclude whether the use of security ratings was predictive of a breach, Marsh McLennan and SecurityScorecard conducted a correlational study to identify the main drivers of cyber risk. ***[See methodology on page 9]***
By analyzing security ratings and cyber insurance incidence data, we found seven factors that have predictive power of a breach and we have listed them in order of highest predictability.

1. ENDPOINT SECURITY
Tracks identification points that are extracted from metadata related to the operating system, web browser, and related active plugins.

2. PATCHING CADENCE
Analyzes how quickly an organization installs security updates to measure vulnerability risk mitigation practices.

3. RANSOMWARE SCORE
Measures how susceptible the organization is to a ransomware attack.

4. NETWORK SECURITY
Checks public datasets for evidence of high risk or insecure open ports within the organization network.

5. DNS HEALTH
Measures the health and configuration of an organization's DNS settings. It validates that no malicious events occurred in the passive DNS history of the organization's network.

6. IP REPUTATION
Makes use of the SecurityScorecard sinkhole infrastructure as well as a blend of OSINT malware feeds and third-party threat intelligence data-sharing partnerships.

7. CUBIT SCORE
Measures a variety of security issues that an organization might have, e.g., check public threat intelligence databases for IP addresses that have been flagged.

All seven of these the factors are within an organization's control when trying to reduce its overall risk and improve its security rating. For instance, keeping all web browsers up to date is one example of good endpoint security. By focusing on these seven areas, a company may be able to reduce its cyber risk, which can result in a higher security rating and potentially a lower cyber insurance quote.

Security ratings are entirely evidence-based; everything is scored on an underlying and transparent observation, based on scans of the entire IPv4 space. Correlated with incidence data, SecurityScorecard factors provide insight that can help insureds focus on areas that need the most attention to reduce their risk exposure (such as active patching cadence, browser and operating system updates, managing DNS, etc). Additionally, insurers can make more informed underwriting and pricing decisions.

SecurityScorecard factors provide insight that can help insureds focus on areas that need the most attention to reduce their risk exposure...

In our analysis, endpoint security was the strongest prediction of a cyber incident. Endpoint security, or endpoint protection, refers to securing endpoints — such as desktops, laptops, and mobile devices — from cybersecurity threats. Endpoints can create entry points to organizational networks which cybercriminals can exploit.

Endpoint security is recognized as particularly problematic by CISA, which issued an alert that identified commonly exploited controls and practices and included best practices to mitigate the issues.

Three actions that may reduce cyber risk and maximize your cyber insurance investment

Organizations should consider taking the following steps to prioritize investments that bolster their security posture:

1 Quantify the effectiveness of your security program

Security ratings are measurable performance indicators that are intuitive and can serve as a common language for communicating. Security leaders can use these factors during executive-level or board meetings to justify spending or demonstrate the value of investments. These metrics can also be used in collaboration with enterprise risk managers to demonstrate their organization's insurability during the cyber insurance procurement process.

2 Incorporate continuous monitoring into your security program

Security ratings provide a real-time view of an organization's cyber risk. All predictive factors identified above can be managed by an organization's security team. As controls tied to those factors are implemented or relevant issues are resolved, the factors will immediately reflect improvements.

3 Create an incident response plan

Have a plan in place to show cyber insurers that your team is prepared to take immediate action towards remediating incidents and mitigating risk. The initial 24 hours after a breach are critical, so it's important to act immediately to stop additional losses, fix lingering vulnerabilities, and notify all affected parties.

By taking these actions, insured organizations may lower their cyber risk by reducing the probability of a cybersecurity incident and prioritize resources that increase the ROI of their security spend.

[7] "Weak Security Controls and Practices Routinely Exploited for Initial Public Access," CISA, May 17, 2022

Conclusion

Security ratings have a dual benefit for insurers and the brokers that act on behalf of insureds. Cyber insurers can use security ratings in their underwriting strategies to more accurately evaluate a company's cyber risk exposure and use that insight to inform risk selection decisions. In addition to providing a way to quantify and assess risk, security ratings go a long way towards augmenting missing or incomplete information on policy application forms by giving all parties a shared view of risk. This can reduce information asymmetry, and change how insureds, brokers, and carriers think about and communicate cyber risk since everyone is speaking a common language. Moreover, security ratings are becoming a bigger part of insurers' profitable growth strategies.

Security ratings and data can offer a transparent, two-sided view so that all interested parties can better understand and measure cyber risk. And being aware of the seven factors most predictive of breaches can inform underwriting strategies and help the industry move towards a more sustainable future. A historical view over at least a year is also important, since most cyber policies are written on a claims-made basis. You do not want to be underwriting a company with an ongoing data breach or other cyber compromise since these can take many months to come to light.

Insureds seeking to gain coverage or reduce their premium can use cybersecurity ratings to monitor and control their risks and improve their overall cybersecurity posture. They can use this information to optimize their cybersecurity investments and allocate them efficiently to identify, protect, detect, respond, and recover from cyber incidents. This will help to drive an efficient risk transfer market that has all parties on the same page. Eventually, this helps make all of us, and the world, a safer place.

Study methodology

The Marsh McLennan Global Cyber Risk Analytics Center conducted the following analysis using data provided by SecurityScorecard and Marsh McLennan. No client data left Marsh McLennan's network.

No one rating factor by itself is likely to be conclusive. In order to discover which factors are statistically significant, two data sets are needed: incident and ratings data. The cyber incident data comes from Marsh McLennan and includes "notice of circumstance" declarations that insured companies make to their insurance carrier in addition to insurable cyber events. This data set covers accidental and adversarial incidents, as well as events that may produce claims. It's worth noting that the data set is relatively sparse, meaning several years of data need to be analyzed to see a statistically significant signal (this study focused on 2019-2021). We enriched the incident data with firmographic data, including North American Industry Classification System (NAICS) industry codes and company revenue. SecurityScorecard supplied the cybersecurity ratings data going back to 2018 and the data set included ratings factors.

Joining the two data sets gave us approximately 12,000 unique entities, with an incident rate of 3.1%. These entities were globally distributed and covered a range of revenues and industries.

Incidents are a binary variable: either we know of an incident or we don't. By contrast, the cybersecurity factor data (which comes from the seven predictive factors mentioned above) is a proportion. For these proportions, the higher they are, the lower the risk, with 1 being the lowest possible risk. To relate the binary to a proportion, we used the rank biserial correlation method which gave us the strength and direction of any correlation.

We synthesized a 95% confidence interval for the correlation coefficient. The correlation coefficient values can range from -1 to +1, with a negative score indicating the factor is predictive of a breach. To be clear, the more negative a correlation is, the more predictive power the factor score has. Obviously, this is a multi-comparison test which we have to correct for, so we applied a family-wise correction to the confidence interval.

We used a simple and very common test for significance: if the 95% confidence interval does not include zero we consider the result statistically significant.

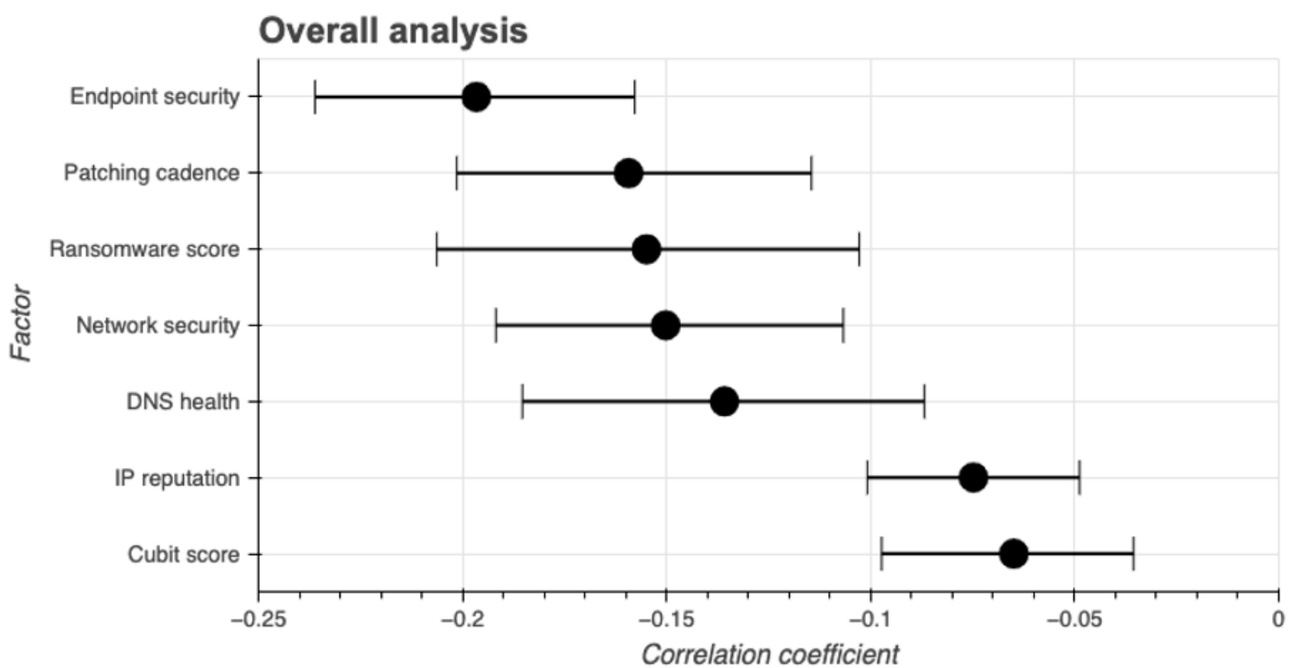
We examined the overall results before breaking down the data set by revenue and industry. Of course, as the number of samples shrinks, the size of the confidence interval increases.

Study methodology

ALL ENTITIES

The chart below shows the 95% confidence interval of the correlation coefficient for all the entities in the study.

Bearing in mind that a correlation of -1 indicates perfect correlation, these results are extremely positive; they suggest these factors have strong predictive power.



Study methodology

REVENUE VARIATIONS

Big companies are not just small companies scaled up; they can be qualitatively different too. To estimate if revenue makes a difference, we sliced up the entities into four annual revenue buckets:

Size	<$100M	$100-$500M	$500-$1B	>$1B
# of companies	8,092	3,062	559	955
Incident rate	1.6%	7%	9.3%	9.9%
Top Factor	**Ransomware Score**	**Endpoint Security**	**N/A - Statistical Noise**	**Endpoint Security**

Study methodology

INDUSTRY VARIATIONS

We examined eight different industry groups using NAICS codes.

Once again, small sample sizes lead to large confidence intervals meaning that for some industry groups the results are not statistically significant.

Given the small sample sizes and the fact this is a multi-comparison test, the different rank ordering of factors isn't that surprising. It's also possible that different industries do have different vulnerabilities; it's well known that industry is a factor in company culture[9], so we might expect similar companies to have similar vulnerabilities. The obvious observation here is that the top factors can be controlled by companies, for example, introducing patching programs, enforcing browser and operating system updates and so on.

Industry	NAICS Code	Sample Size	Incident Rate	Top Predictive Factors
Manufacturing	31- 33	1,487	2.97%	1. Ransomware Score 2. Network Security 3. Patching Cadence
Retail Trade	44-45	521	3.81%	1. Endpoint Security
Information	51	516	4.92%	1. Endpoint Security 2. IP Reputation
Real Estate Rental & Leasing	53	322	2.22%	1. Patching Cadence 2. Ransomware Score 3. Network Security
Professional, Scientific, & Technical Services	54	2,173	2.94%	1. DNS Health 2. Endpoint Security 3. Network Security 4. Patching Cadence
Education Services	61	749	6.10%	1. Endpoint Security 2. Patching Cadence
Health Care & Social Assistance	62	801	5.01%	1. Endpoint Security
Arts, Entertainment, and Recreation[8]	71	172	3.79	1. Total Score 2. Patching Cadence 3. Network Security

[8] "Why Cyber Attacks Against Film And Media Industries Are Escalating", Forbes https://www.forbes.com/sites/davidbalaban/2021/06/11/why-cyber-attacks-against-film-and-media-industries-are-escalating

[9] Christensen, E. W., & Gordon, G. G. (1999). "An exploration of industry, culture, and revenue growth". Organization studies , 397-42

About SecurityScorecard

Funded by world-class investors including Evolution Equity Partners, Silver Lake Waterman, 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 30,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight. SecurityScorecard is the first cybersecurity ratings company to offer digital forensics and incident response services, providing a 360-degree approach to security prevention and response for its worldwide customer and partner base.

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**.

Create your FREE account today.
Prepare, defend, and respond to cyber risk with trusted advisors.

GET STARTED

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.com

United States: (800) 682-1701
International: +1(646) 809-2166

About Marsh McLennan

Marsh McLennan (NYSE: MMC) is the world's leading professional services firm in the areas of risk, strategy and people. The Company's more than 85,000 colleagues advise clients in 130 countries. With annual revenue of over $20 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses. **Marsh** provides data-driven risk advisory services and insurance solutions to commercial and consumer clients. **Guy Carpenter** develops advanced risk, reinsurance and capital strategies that help clients grow profitably and pursue emerging opportunities. **Mercer** delivers advice and technology-driven solutions that help organizations redefine the world of work, reshape retirement and investment outcomes, and unlock health and wellbeing for a changing workforce. **Oliver Wyman** serves as a critical strategic, economic and brand advisor to private sector and governmental clients. For more information, visit **marshmclennan.com** and follow us on **LinkedIn** and **Twitter**.

MarshMcLennan

Marshmclennan.com