Cyberwrite

AI-DRIVEN CYBER INSURANCE TECHNOLOGIES

www.cyberwrite.com

ABOUT CYBERWRITE

Founded in 2017 by industry veterans.

Developed the 4SEEN AI technology for cyber insurance underwriting, sales, and aggregated risk management.

Serves the world's largest insurance and reinsurance groups.

Over **$20 Billion** limit of cyber insurance risk is analyzed using the Cyberwrite platform.

Example Customers

Munich RE

CINCINNATI FINANCIAL CORPORATION

MAPFRE

CRC

1866 Hartford Steam Boiler

MARKEL

TRUIST

howden

DUAL

Cyber Insurance

SINGLE LARGEST OPPORTUNITY FOR GROWTH

By 2030 – $50bn in Annual Premiums

Source: Howden

CYBER INSURANCE

CHALLENGES OF REINSURERS AND INSURERS

Lack of visibility into the actual insureds in some cases

Insufficient claims data

Insufficient risk data on small and mid-market.

Vast amounts of data on corporates

Very hard to make sense out of if you are not a cyber security expert!

The opportunity of Using AI

ENABLE UNDERWRITERS!

“Some computers have now crossed

the exascale threshold, meaning that they can perform as many calculations in a single second as an individual could in 31,688,765,000 years.”

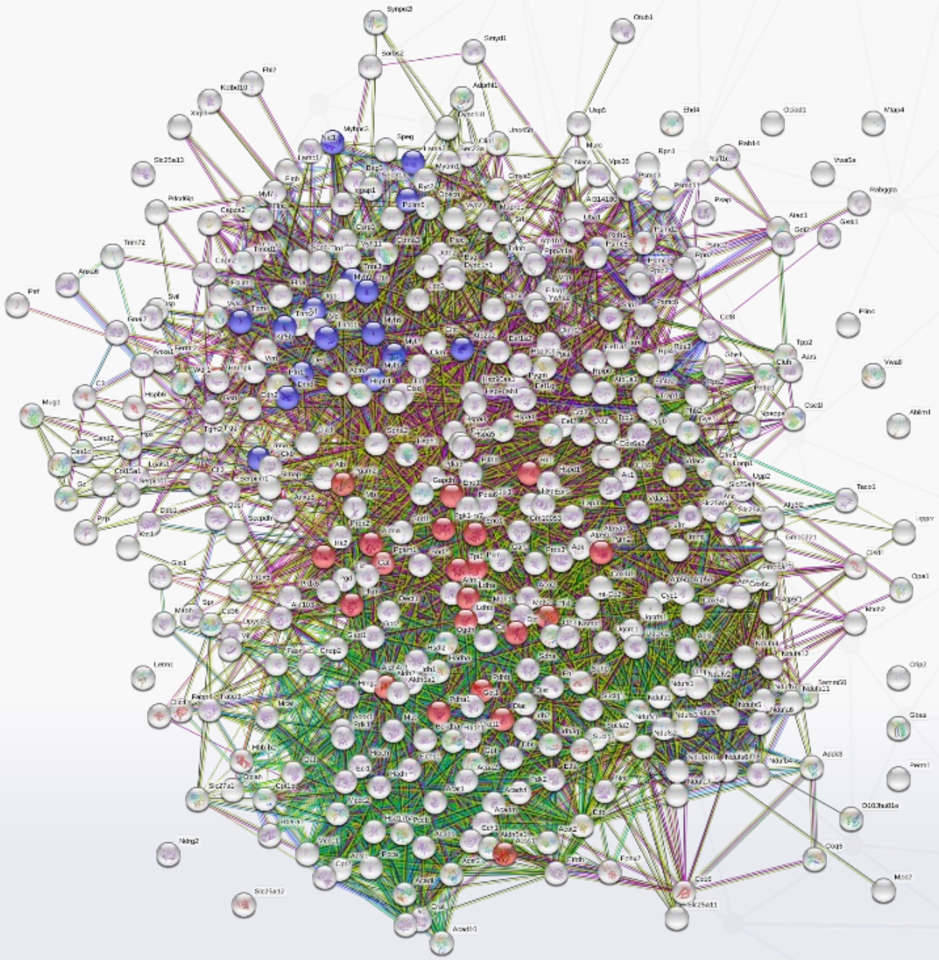
Source: McKinsey

https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-ai

DATA IN INSURANCE

On one end – not enough data – and on the other hand **too much data for a human to digest** during underwriting

Each dot is a cyber data point, and the underwriter needs to make sense out of it – it’s tough to achieve.



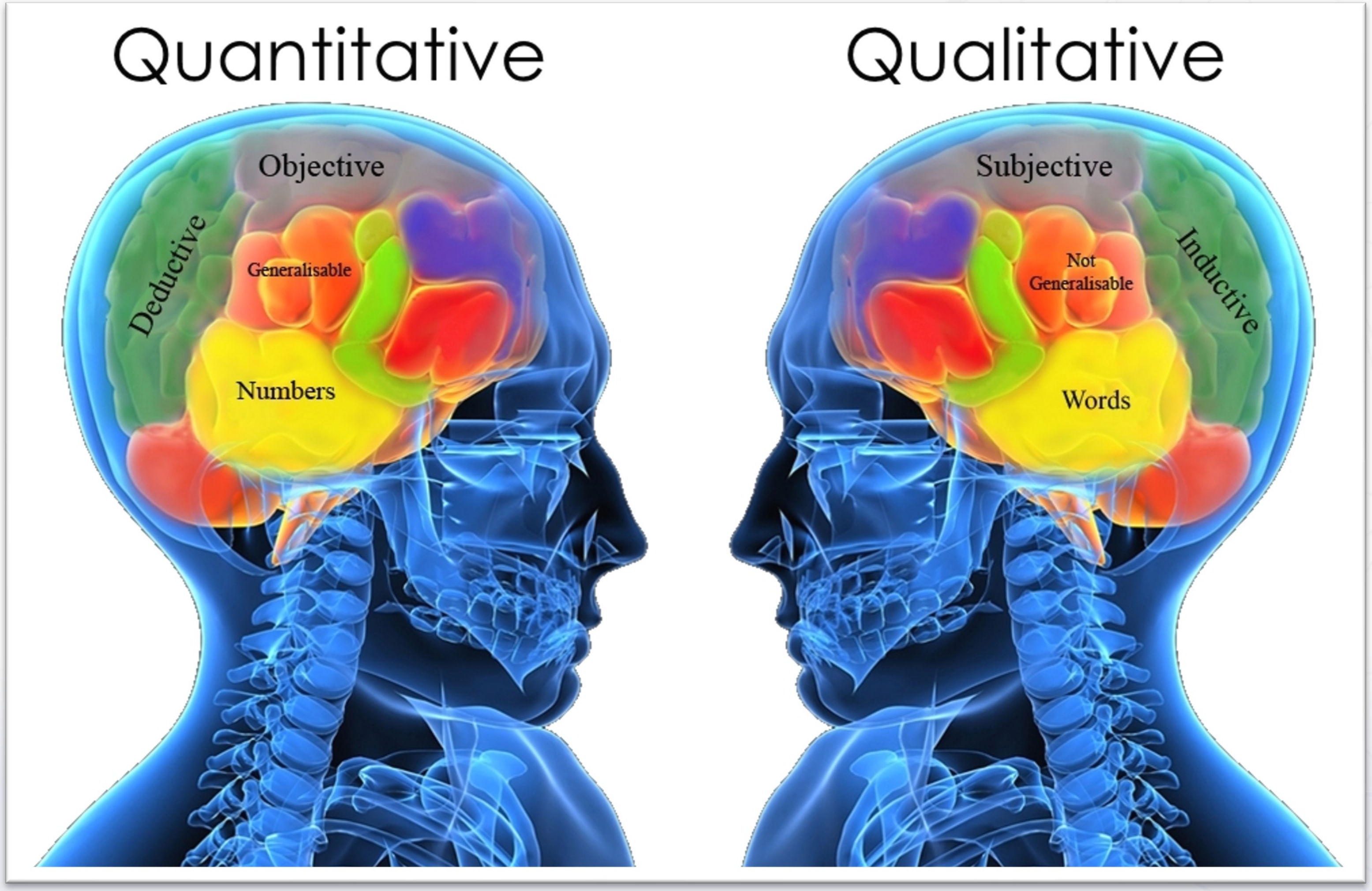
AI & UNDERWRITING

HOW TO BRIDGE THIS GAP

Quantitative, not Qualitative

High Risk, Low Risk

Remove the Underwriting Bias from the equation



Based On over 500+ meetings

with Carriers, Brokers, and reinsurers, the following pain points have been identified:

High Risk, Low Risk

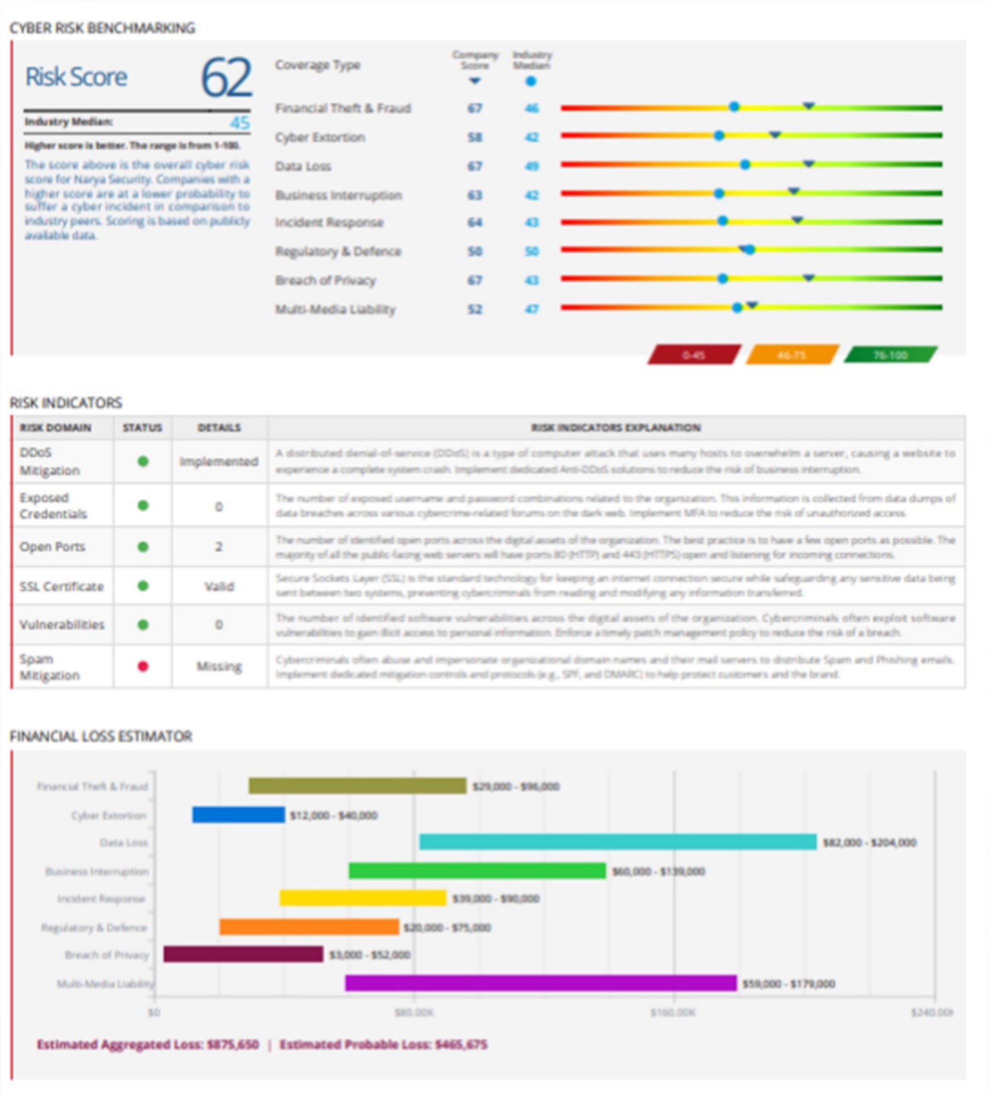
- Underwriters need AI to analyze data
- Brokers need AI to enable them to effectively explain risk
- Insureds need to use AI to reduce risk
- Reinsurers can use AI to analyze book risk

A report for any company within seconds (Using SAAS or API).

Inherent and residual risk analysis for each coverage with industry benchmark

Highlights and key findings based on external data collection

Estimated economic impact for each coverage, tailored to each organization



CYBER RISK BENCHMARKING

Risk Score 62

Industry Median: 45

Higher score is better. The range is from 1-100.

The score above is the overall cyber risk score for Narya Security. Companies with a higher score are at a lower probability to suffer a cyber incident in comparison to industry peers. Scoring is based on publicly available data.

Coverage Type	Company Score	Industry Median
Financial Theft & Fraud	67	46
Cyber Extortion	58	42
Data Loss	67	49
Business Interruption	63	42
Incident Response	64	43
Regulatory & Defence	50	50
Breach of Privacy	67	43
Multi-Media Liability	52	47

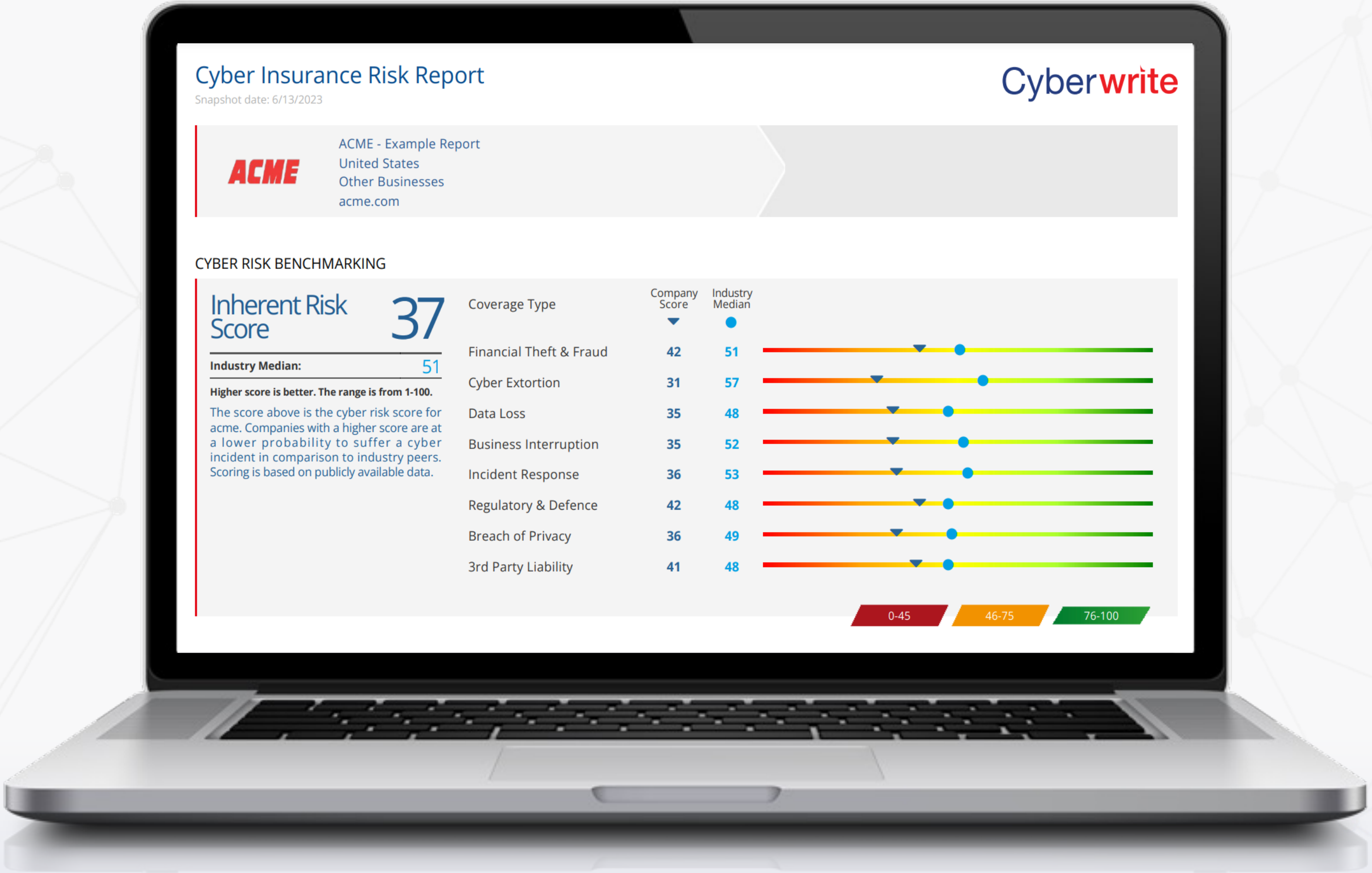
RISK INDICATORS

RISK DOMAIN	STATUS	DETAILS	RISK INDICATORS EXPLANATION
DDoS Mitigation	●	Implemented	A distributed denial-of-service (DDoS) is a type of computer attack that uses many hosts to overwhelm a server, causing a website to experience a complete system crash. Implement dedicated Anti-DDoS solutions to reduce the risk of business interruption.
Exposed Credentials	●	0	The number of exposed username and password combinations related to the organization. This information is collected from data dumps of data breaches across various cybercrime-related forums on the dark web. Implement MFA to reduce the risk of unauthorized access.
Open Ports	●	2	The number of identified open ports across the digital assets of the organization. The best practice is to have a few open ports as possible. The majority of all the public-facing web servers will have ports 80 (HTTP) and 443 (HTTPS) open and listening for incoming connections.
SSL Certificate	●	Valid	Secure Sockets Layer (SSL) is the standard technology for keeping an internet connection secure while safeguarding any sensitive data being sent between two systems, preventing cybercriminals from reading and modifying any information transferred.
Vulnerabilities	●	0	The number of identified software vulnerabilities across the digital assets of the organization. Cybercriminals often exploit software vulnerabilities to gain illicit access to personal information. Enforce a timely patch management policy to reduce the risk of a breach.
Spam Mitigation	●	Missing	Cybercriminals often abuse and impersonate organizational domain names and their mail servers to distribute Spam and Phishing emails. Implement dedicated mitigation controls and protocols (e.g., SPF, and DMARC) to help protect customers and the brand.

FINANCIAL LOSS ESTIMATOR

Estimated Aggregated Loss: $875,650 | Estimated Probable Loss: $465,675

Since 2017, we have had over 99.97% coverage globally! Access risk data of over 100 Million companies



Cyber Insurance Risk Report

Snapshot date: 6/13/2023

Cyberwrite

ACME

ACME - Example Report
United States
Other Businesses
acme.com

CYBER RISK BENCHMARKING

Inherent Risk Score 37

Industry Median: 51

Higher score is better. The range is from 1-100.

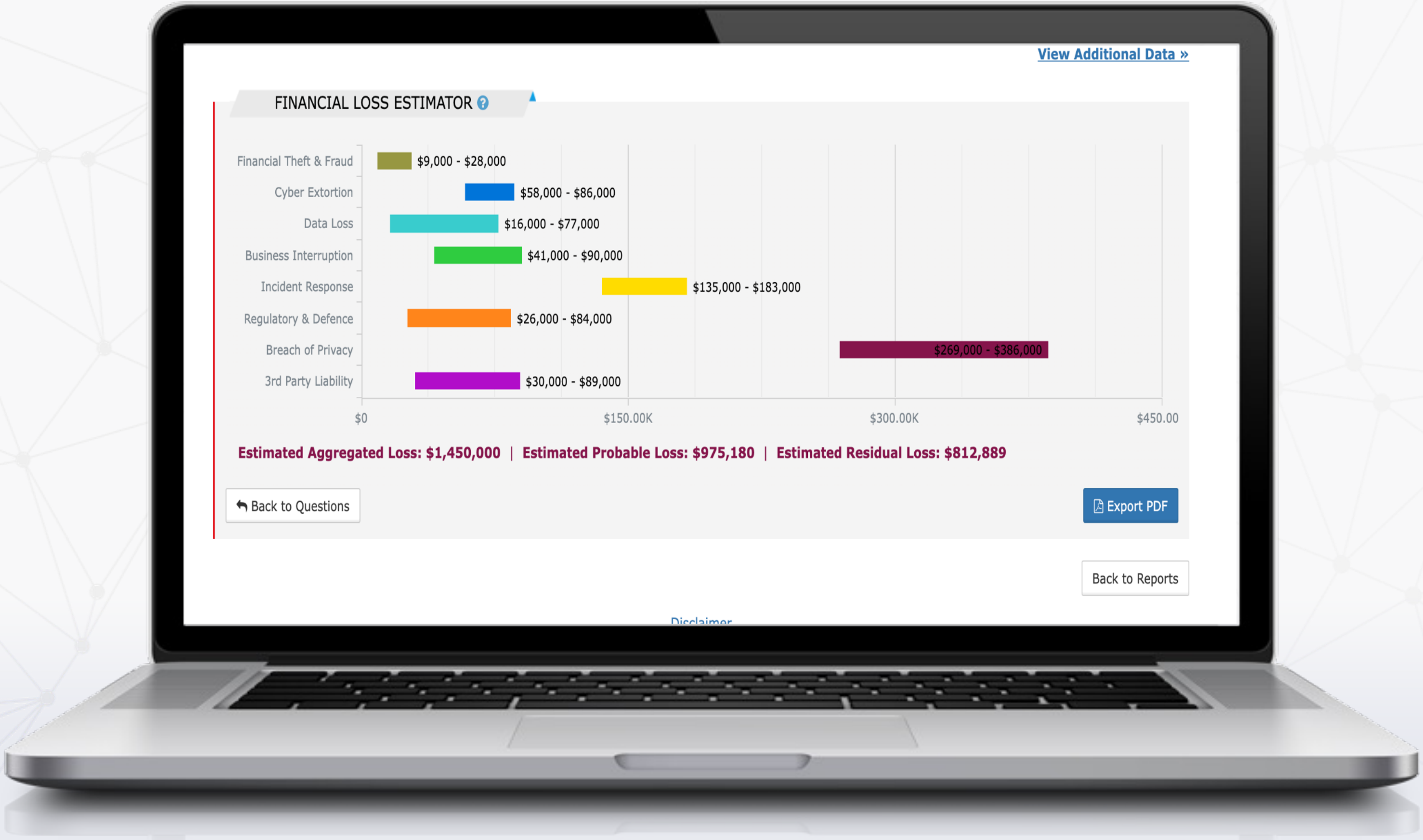
The score above is the cyber risk score for acme. Companies with a higher score are at a lower probability to suffer a cyber incident in comparison to industry peers. Scoring is based on publicly available data.

Coverage Type	Company Score ▼	Industry Median ●
Financial Theft & Fraud	42	51
Cyber Extortion	31	57
Data Loss	35	48
Business Interruption	35	52
Incident Response	36	53
Regulatory & Defence	42	48
Breach of Privacy	36	49
3rd Party Liability	41	48

🟥 0-45 🟧 46-75 🟩 76-100

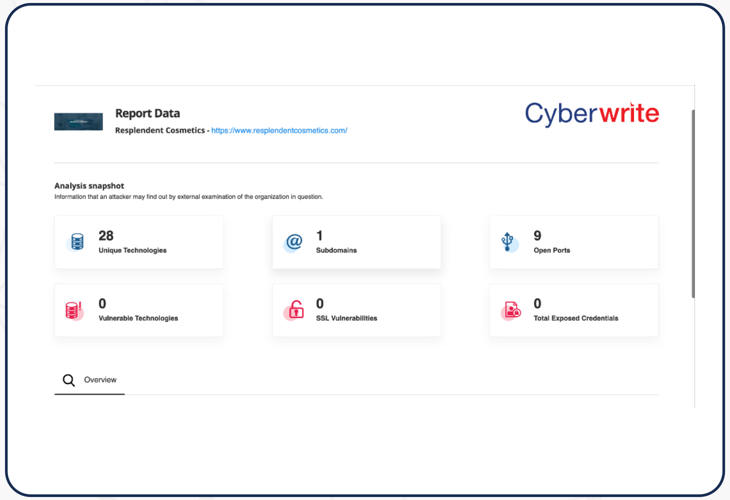
Also Available in multiple languages in addition to English (German, French, Spanish, Portuguese, Japanese, Italian)

ECONOMIC IMPACT ANALYSIS OF ANY BUSINESS IN REAL-TIME DRIVES ADOPTION AND AWARENESS



Estimated Aggregated Loss: $1,450,000 | Estimated Probable Loss: $975,180 | Estimated Residual Loss: $812,889

IN-DEPTH CYBER RISK INSIGHTS ON ANY COMPANY (EXAMPLE SCREENSHOTS)



Report Data

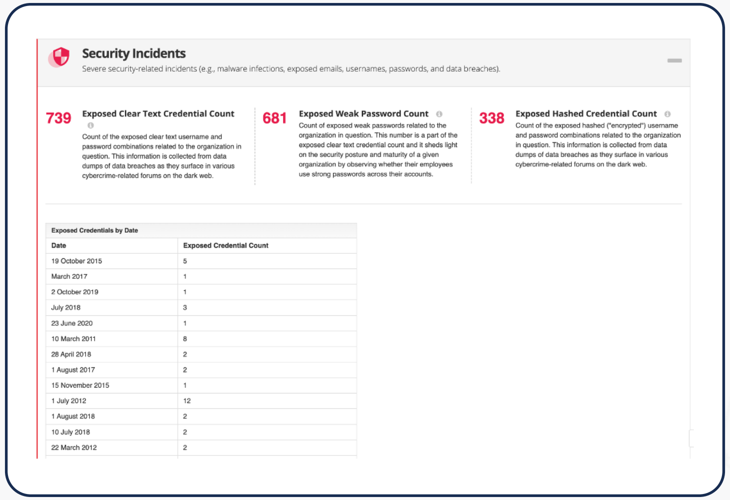
Resplendent Cosmetics - https://www.resplendentcosmetics.com/

Cyberwrite

Analysis snapshot

Information that an attacker may find out by external examination of the organization in question.

28 Unique Technologies	1 Subdomains	9 Open Ports
0 Vulnerable Technologies	0 SSL Vulnerabilities	0 Total Exposed Credentials



Security Incidents

Severe security-related incidents (e.g., malware infections, exposed emails, usernames, passwords, and data breaches).

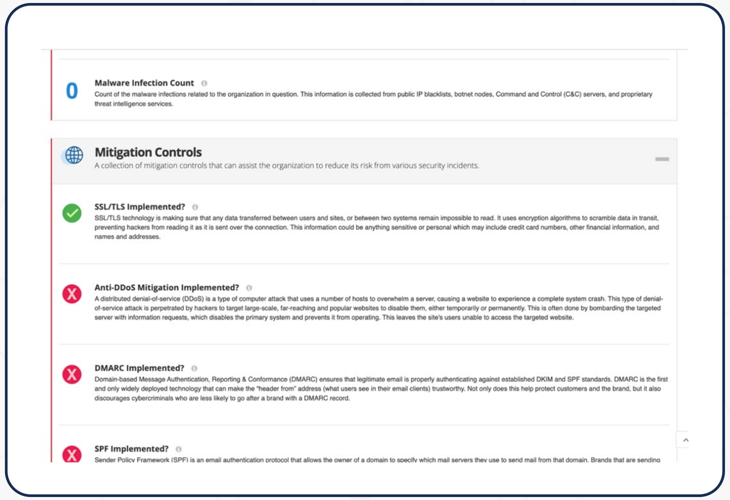
739 **Exposed Clear Text Credential Count**
Count of the exposed clear text username and password combinations related to the organization in question. This information is collected from data dumps of data breaches as they surface in various cybercrime-related forums on the dark web.

681 **Exposed Weak Password Count**
Count of exposed weak passwords related to the organization in question. This number is a part of the exposed clear text credential count and it sheds light on the security posture and maturity of a given organization by observing whether their employees use strong passwords across their accounts.

338 **Exposed Hashed Credential Count**
Count of the exposed hashed ("encrypted") username and password combinations related to the organization in question. This information is collected from data dumps of data breaches as they surface in various cybercrime-related forums on the dark web.

Exposed Credentials by Date

Date	Exposed Credential Count
19 October 2015	5
March 2017	1
2 October 2019	1
July 2018	3
23 June 2020	1
10 March 2011	8
28 April 2018	2
1 August 2017	2
15 November 2015	1
1 July 2012	12
1 August 2018	2
10 July 2018	2
22 March 2012	2



0 **Malware Infection Count**
Count of the malware infections related to the organization in question. This information is collected from public IP blacklists, botnet nodes, Command and Control (C&C) servers, and proprietary threat intelligence services.

Mitigation Controls

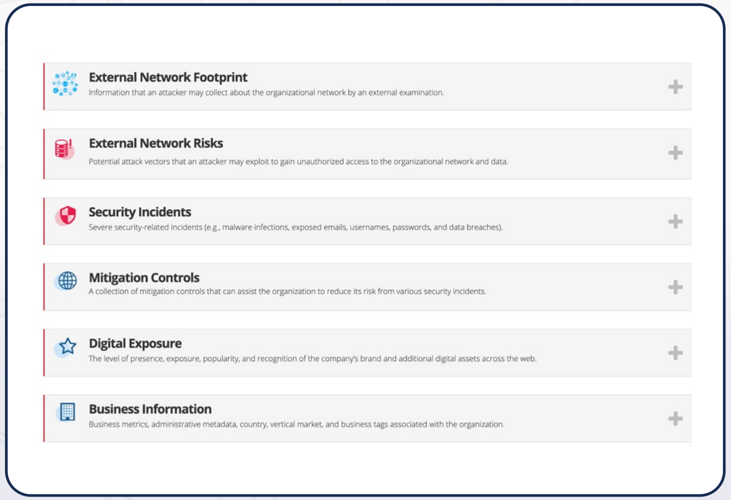
A collection of mitigation controls that can assist the organization to reduce its risk from various security incidents.

✓ **SSL/TLS Implemented?**
SSL/TLS technology is making sure that any data transferred between users and sites, or between two systems remain impossible to read. It uses encryption algorithms to scramble data in transit, preventing hackers from reading it as it is sent over the connection. This information could be anything sensitive or personal which may include credit card numbers, other financial information, and names and addresses.

☒ **Anti-DDoS Mitigation Implemented?**
A distributed denial-of-service (DDoS) is a type of computer attack that uses a number of hosts to overwhelm a server, causing a website to experience a complete system crash. This type of denial-of-service attack is perpetrated by hackers to target large-scale, far-reaching and popular websites to disable them, either temporarily or permanently. This is often done by bombarding the targeted server with information requests, which disables the primary system and prevents it from operating. This leaves the site's users unable to access the targeted website.

☒ **DMARC Implemented?**
Domain-based Message Authentication, Reporting & Conformance (DMARC) ensures that legitimate email is properly authenticating against established DKIM and SPF standards. DMARC is the first and only widely deployed technology that can make the "header from" address (what users see in their email clients) trustworthy. Not only does this help protect customers and the brand, but it also discourages cybercriminals who are less likely to go after a brand with a DMARC record.

☒ **SPF Implemented?**
Sender Policy Framework (SPF) is an email authentication protocol that allows the owner of a domain to specify which mail servers they use to send mail from that domain. Brands that are sending



External Network Footprint +
Information that an attacker may collect about the organizational network by an external examination.

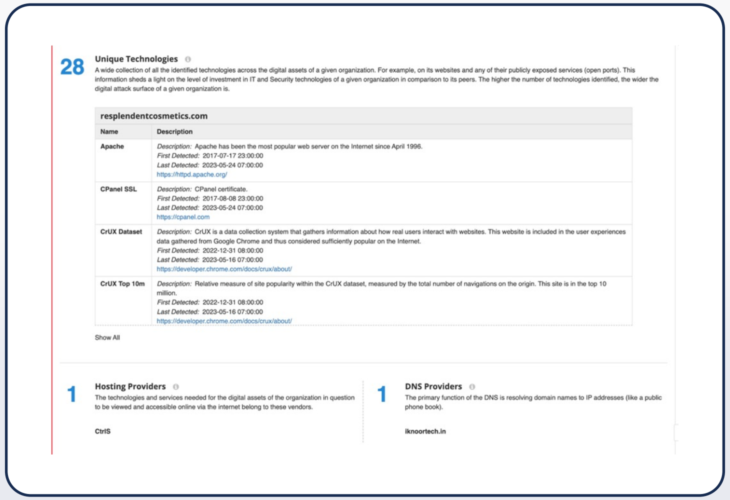
External Network Risks +
Potential attack vectors that an attacker may exploit to gain unauthorized access to the organizational network and data.

Security Incidents +
Severe security-related incidents (e.g., malware infections, exposed emails, usernames, passwords, and data breaches).

Mitigation Controls +
A collection of mitigation controls that can assist the organization to reduce its risk from various security incidents.

Digital Exposure +
The level of presence, exposure, popularity, and recognition of the company's brand and additional digital assets across the web.

Business Information +
Business metrics, administrative metadata, country, vertical market, and business tags associated with the organization.



28 **Unique Technologies**
A wide collection of all the identified technologies across the digital assets of a given organization. For example, on its websites and any of their publicly exposed services (open ports). This information sheds a light on the level of investment in IT and Security technologies of a given organization in comparison to its peers. The higher the number of technologies identified, the wider the digital attack surface of a given organization is.

resplendentcosmetics.com

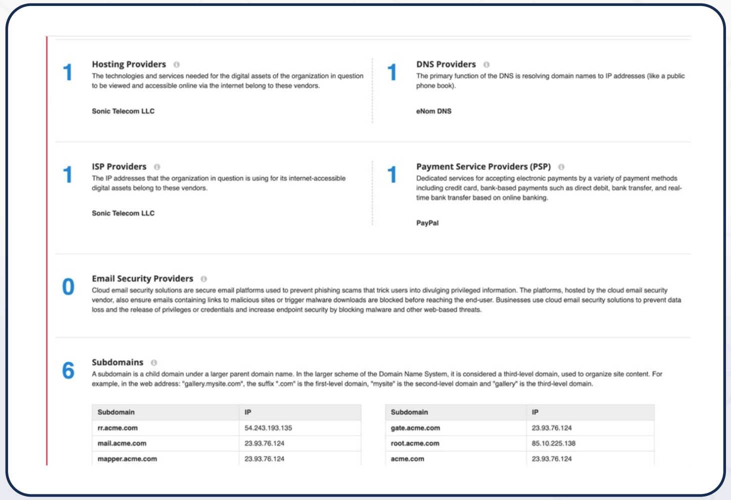
Name	Description
Apache	*Description:* Apache has been the most popular web server on the Internet since April 1996. *First Detected:* 2017-07-17 23:00:00 *Last Detected:* 2023-05-24 07:00:00 https://httpd.apache.org/
CPanel SSL	*Description:* CPanel certificate. *First Detected:* 2017-08-08 23:00:00 *Last Detected:* 2023-05-24 07:00:00 https://cpanel.com
CrUX Dataset	*Description:* CrUX is a data collection system that gathers information about how real users interact with websites. This website is included in the user experiences data gathered from Google Chrome and thus considered sufficiently popular on the Internet. *First Detected:* 2022-12-31 08:00:00 *Last Detected:* 2023-05-16 07:00:00 https://developer.chrome.com/docs/crux/about/
CrUX Top 10m	*Description:* Relative measure of site popularity within the CrUX dataset, measured by the total number of navigations on the origin. This site is in the top 10 million. *First Detected:* 2022-12-31 08:00:00 *Last Detected:* 2023-05-16 07:00:00 https://developer.chrome.com/docs/crux/about/

1 **Hosting Providers**
The technologies and services needed for the digital assets of the organization in question to be viewed and accessible online via the internet belong to these vendors.

CtrlS

1 **DNS Providers**
The primary function of the DNS is resolving domain names to IP addresses (like a public phone book).

iknoortech.in



1 **Hosting Providers**
The technologies and services needed for the digital assets of the organization in question to be viewed and accessible online via the internet belong to these vendors.

Sonic Telecom LLC

1 **DNS Providers**
The primary function of the DNS is resolving domain names to IP addresses (like a public phone book).

eNom DNS

1 **ISP Providers**
The IP addresses that the organization in question is using for its internet-accessible digital assets belong to these vendors.

Sonic Telecom LLC

1 **Payment Service Providers (PSP)**
Dedicated services for accepting electronic payments by a variety of payment methods including credit card, bank-based payments such as direct debit, bank transfer, and real-time bank transfer based on online banking.

PayPal

0 **Email Security Providers**
Cloud email security solutions are secure email platforms used to prevent phishing scams that trick users into divulging privileged information. The platforms, hosted by the cloud email security vendor, also ensure emails containing links to malicious sites or trigger malware downloads are blocked before reaching the end-user. Businesses use cloud email security solutions to prevent data loss and the release of privileges or credentials and increase endpoint security by blocking malware and other web-based threats.

6 **Subdomains**
A subdomain is a child domain under a larger parent domain name. In the larger scheme of the Domain Name System, it is considered a third-level domain, used to organize site content. For example, in the web address: "gallery.mysite.com", the suffix ".com" is the first-level domain, "mysite" is the second-level domain and "gallery" is the third-level domain.

Subdomain	IP
rr.acme.com	54.243.193.135
mail.acme.com	23.93.76.124
mapper.acme.com	23.93.76.124

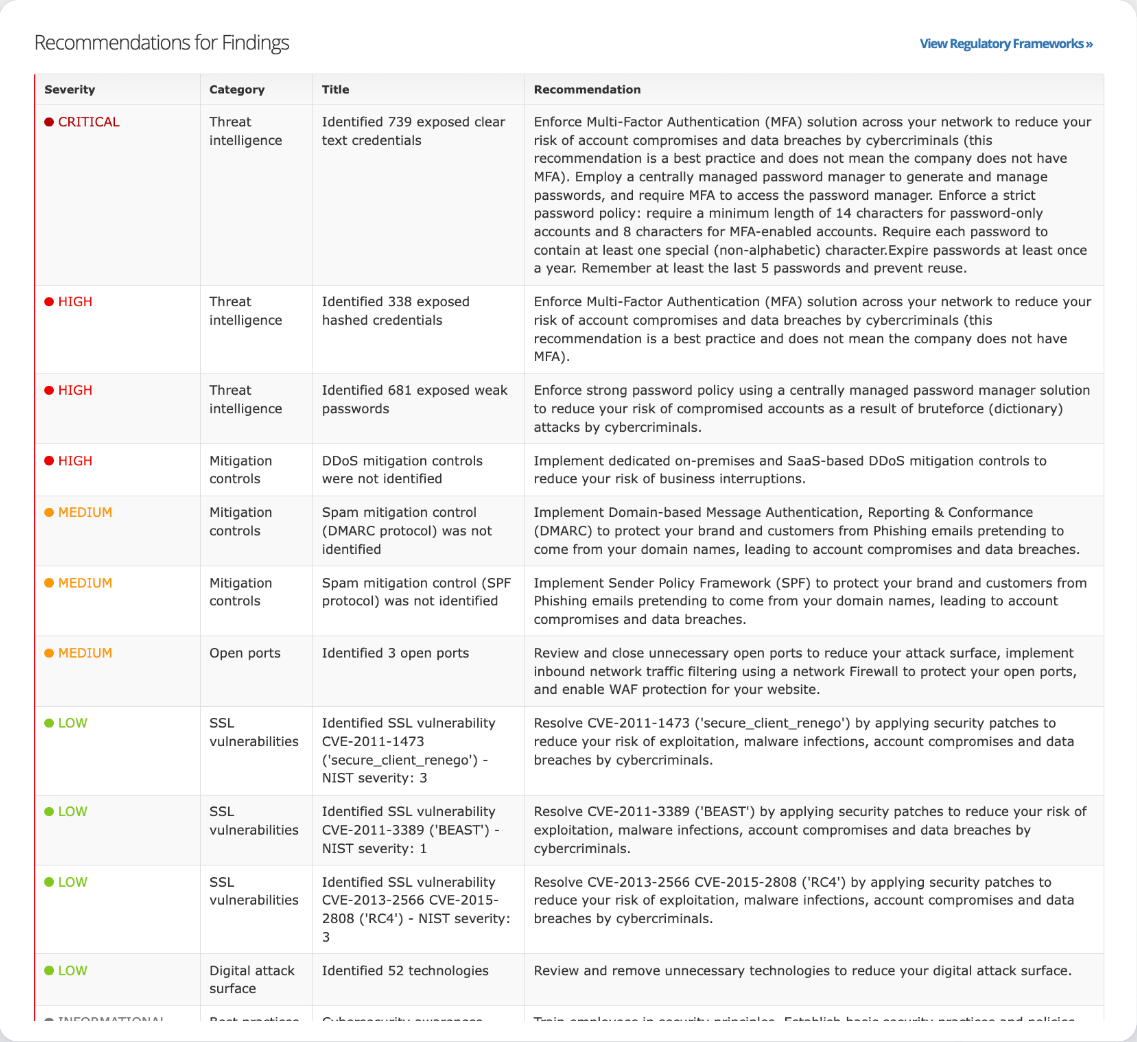
Subdomain	IP
gate.acme.com	23.93.76.124
root.acme.com	85.10.225.138
acme.com	23.93.76.124

RISK REDUCTION RECOMMENDATIONS FOR BUSINESSES

Actionable recommendations the insured may use to proactively mitigate the risk based on the data findings.

Each recommendation is prioritized to save time and enable to focus on the most important issues

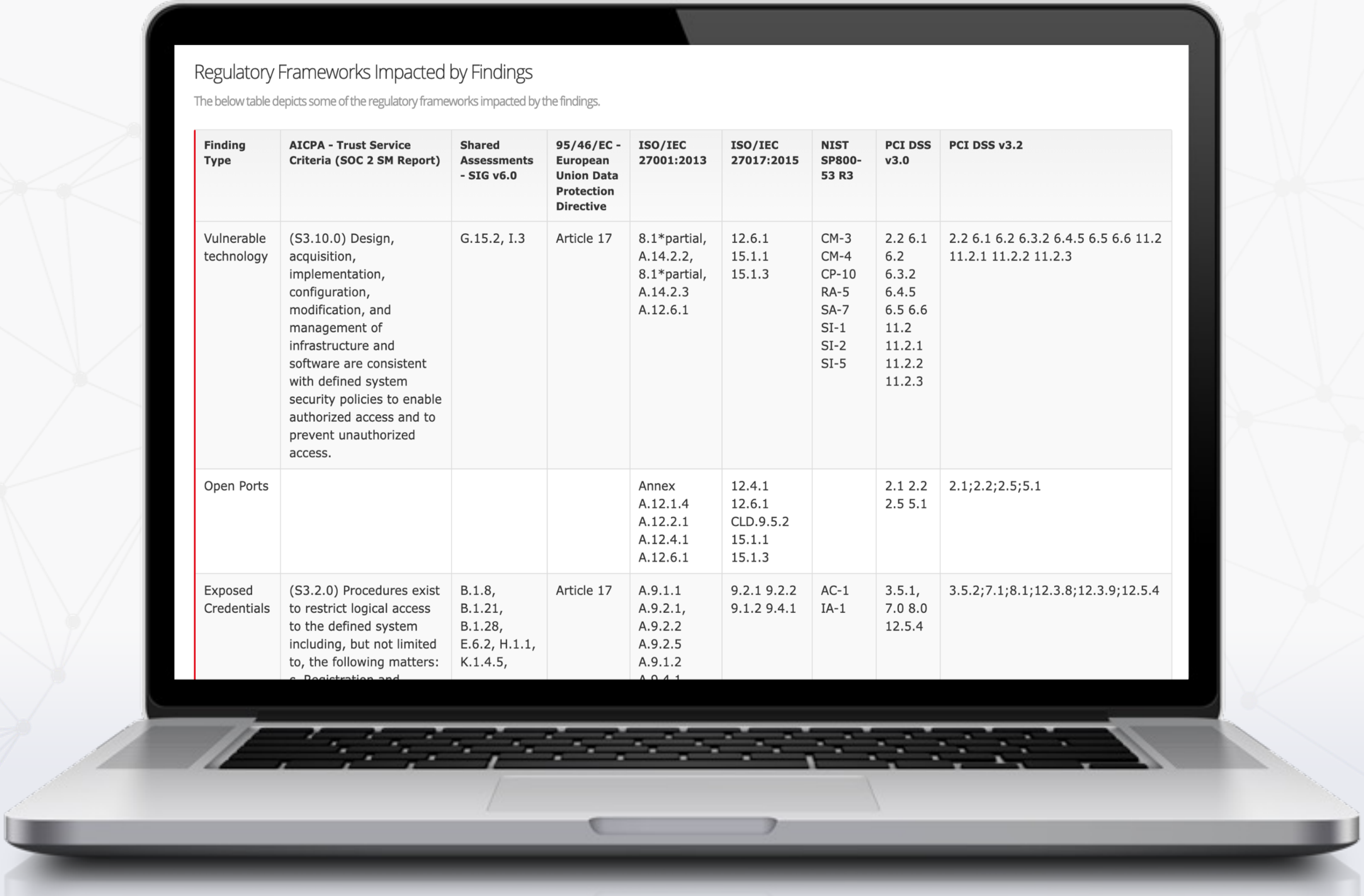
The report is sent to the broker, which delivers it to the customer either in a PDF or on a dedicated portal.



Recommendations for Findings

Severity	Category	Title	Recommendation
● CRITICAL	Threat intelligence	Identified 739 exposed clear text credentials	Enforce Multi-Factor Authentication (MFA) solution across your network to reduce your risk of account compromises and data breaches by cybercriminals (this recommendation is a best practice and does not mean the company does not have MFA). Employ a centrally managed password manager to generate and manage passwords, and require MFA to access the password manager. Enforce a strict password policy: require a minimum length of 14 characters for password-only accounts and 8 characters for MFA-enabled accounts. Require each password to contain at least one special (non-alphabetic) character.Expire passwords at least once a year. Remember at least the last 5 passwords and prevent reuse.
● HIGH	Threat intelligence	Identified 338 exposed hashed credentials	Enforce Multi-Factor Authentication (MFA) solution across your network to reduce your risk of account compromises and data breaches by cybercriminals (this recommendation is a best practice and does not mean the company does not have MFA).
● HIGH	Threat intelligence	Identified 681 exposed weak passwords	Enforce strong password policy using a centrally managed password manager solution to reduce your risk of compromised accounts as a result of bruteforce (dictionary) attacks by cybercriminals.
● HIGH	Mitigation controls	DDoS mitigation controls were not identified	Implement dedicated on-premises and SaaS-based DDoS mitigation controls to reduce your risk of business interruptions.
● MEDIUM	Mitigation controls	Spam mitigation control (DMARC protocol) was not identified	Implement Domain-based Message Authentication, Reporting & Conformance (DMARC) to protect your brand and customers from Phishing emails pretending to come from your domain names, leading to account compromises and data breaches.
● MEDIUM	Mitigation controls	Spam mitigation control (SPF protocol) was not identified	Implement Sender Policy Framework (SPF) to protect your brand and customers from Phishing emails pretending to come from your domain names, leading to account compromises and data breaches.
● MEDIUM	Open ports	Identified 3 open ports	Review and close unnecessary open ports to reduce your attack surface, implement inbound network traffic filtering using a network Firewall to protect your open ports, and enable WAF protection for your website.
● LOW	SSL vulnerabilities	Identified SSL vulnerability CVE-2011-1473 ('secure_client_renego') - NIST severity: 3	Resolve CVE-2011-1473 ('secure_client_renego') by applying security patches to reduce your risk of exploitation, malware infections, account compromises and data breaches by cybercriminals.
● LOW	SSL vulnerabilities	Identified SSL vulnerability CVE-2011-3389 ('BEAST') - NIST severity: 1	Resolve CVE-2011-3389 ('BEAST') by applying security patches to reduce your risk of exploitation, malware infections, account compromises and data breaches by cybercriminals.
● LOW	SSL vulnerabilities	Identified SSL vulnerability CVE-2013-2566 CVE-2015-2808 ('RC4') - NIST severity: 3	Resolve CVE-2013-2566 CVE-2015-2808 ('RC4') by applying security patches to reduce your risk of exploitation, malware infections, account compromises and data breaches by cybercriminals.
● LOW	Digital attack surface	Identified 52 technologies	Review and remove unnecessary technologies to reduce your digital attack surface.
● INFORMATIONAL	Best practices	Cybersecurity awareness	Train employees in security principles. Establish basic security practices and policies

REGULATORY IMPACT ANALYSIS IS PART OF ANY REPORT TO DRIVE RISK REDUCTION ACTIONS BY INSUREDS

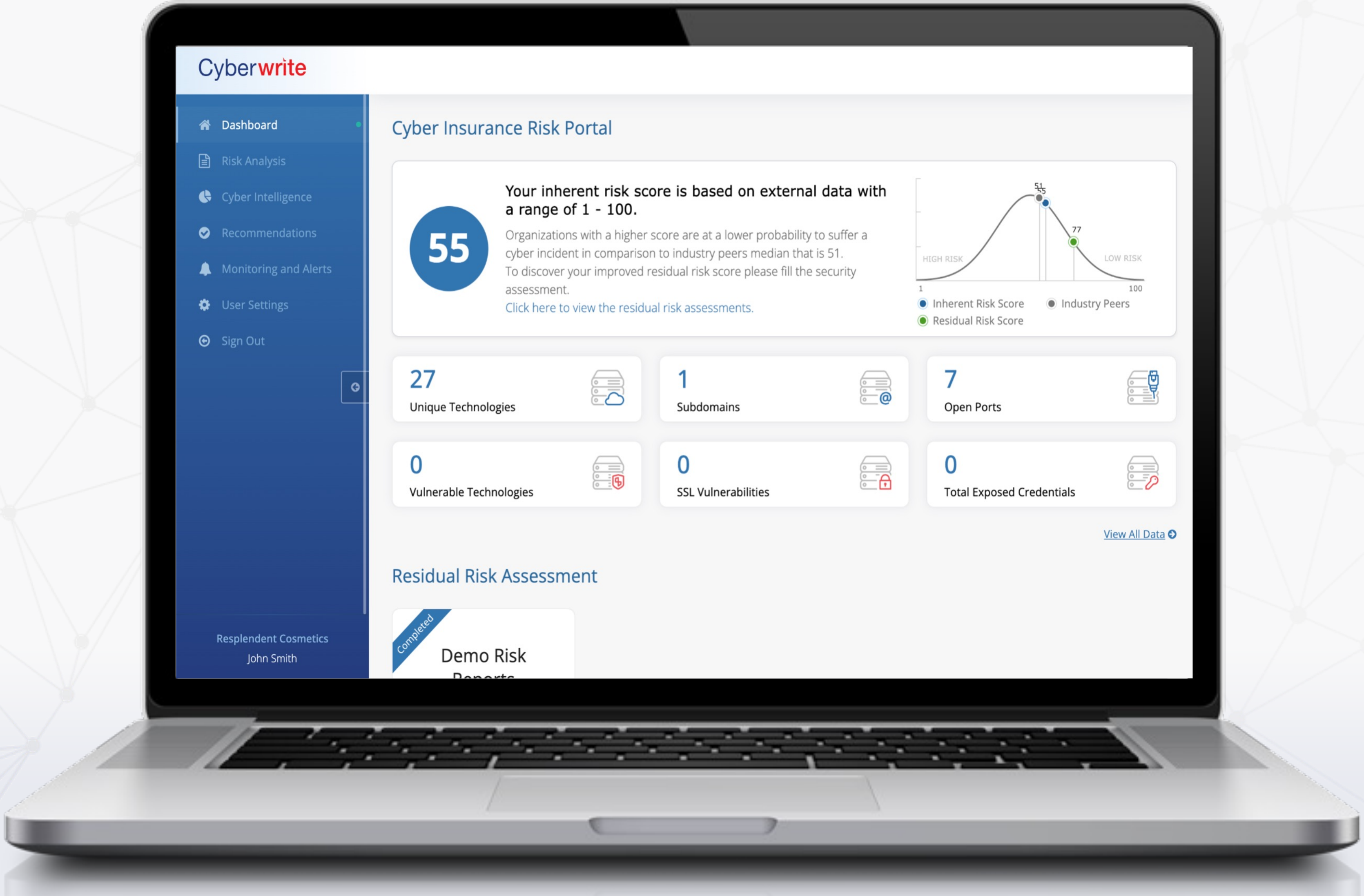


Regulatory Frameworks Impacted by Findings

The below table depicts some of the regulatory frameworks impacted by the findings.

Finding Type	AICPA - Trust Service Criteria (SOC 2 SM Report)	Shared Assessments - SIG v6.0	95/46/EC - European Union Data Protection Directive	ISO/IEC 27001:2013	ISO/IEC 27017:2015	NIST SP800-53 R3	PCI DSS v3.0	PCI DSS v3.2
Vulnerable technology	(S3.10.0) Design, acquisition, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.	G.15.2, I.3	Article 17	8.1*partial, A.14.2.2, 8.1*partial, A.14.2.3 A.12.6.1	12.6.1 15.1.1 15.1.3	CM-3 CM-4 CP-10 RA-5 SA-7 SI-1 SI-2 SI-5	2.2 6.1 6.2 6.3.2 6.4.5 6.5 6.6 11.2 11.2.1 11.2.2 11.2.3	2.2 6.1 6.2 6.3.2 6.4.5 6.5 6.6 11.2 11.2.1 11.2.2 11.2.3
Open Ports				Annex A.12.1.4 A.12.2.1 A.12.4.1 A.12.6.1	12.4.1 12.6.1 CLD.9.5.2 15.1.1 15.1.3		2.1 2.2 2.5 5.1	2.1;2.2;2.5;5.1
Exposed Credentials	(S3.2.0) Procedures exist to restrict logical access to the defined system including, but not limited to, the following matters: c. Registration and	B.1.8, B.1.21, B.1.28, E.6.2, H.1.1, K.1.4.5,	Article 17	A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.5 A.9.1.2 A.9.4.1	9.2.1 9.2.2 9.1.2 9.4.1	AC-1 IA-1	3.5.1, 7.0 8.0 12.5.4	3.5.2;7.1;8.1;12.3.8;12.3.9;12.5.4

INSURED PORTAL FOR DIRECT ACCESS



Cyberwrite

- Dashboard
- Risk Analysis
- Cyber Intelligence
- Recommendations
- Monitoring and Alerts
- User Settings
- Sign Out

Resplendent Cosmetics
John Smith

Cyber Insurance Risk Portal

55

Your inherent risk score is based on external data with a range of 1 - 100.

Organizations with a higher score are at a lower probability to suffer a cyber incident in comparison to industry peers median that is 51.
To discover your improved residual risk score please fill the security assessment.
Click here to view the residual risk assessments.

27 Unique Technologies	1 Subdomains	7 Open Ports
0 Vulnerable Technologies	0 SSL Vulnerabilities	0 Total Exposed Credentials

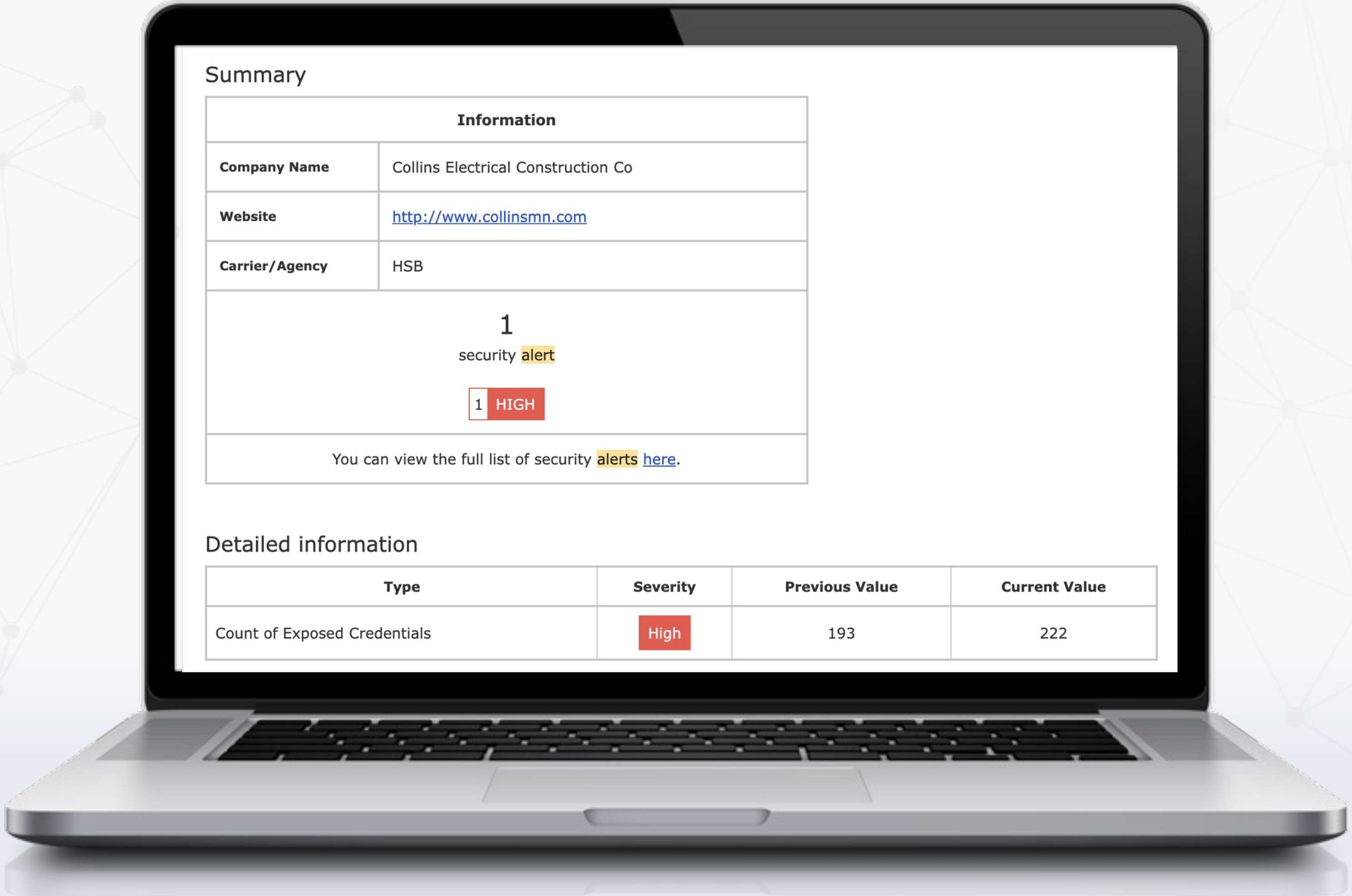
View All Data

Residual Risk Assessment

Completed

Demo Risk
Reports

ONGOING MONITORING AND ALERTS TO CARRIER & INSURED



Summary

Information	
Company Name	Collins Electrical Construction Co
Website	http://www.collinsmn.com
Carrier/Agency	HSB

1

security alert

1 HIGH

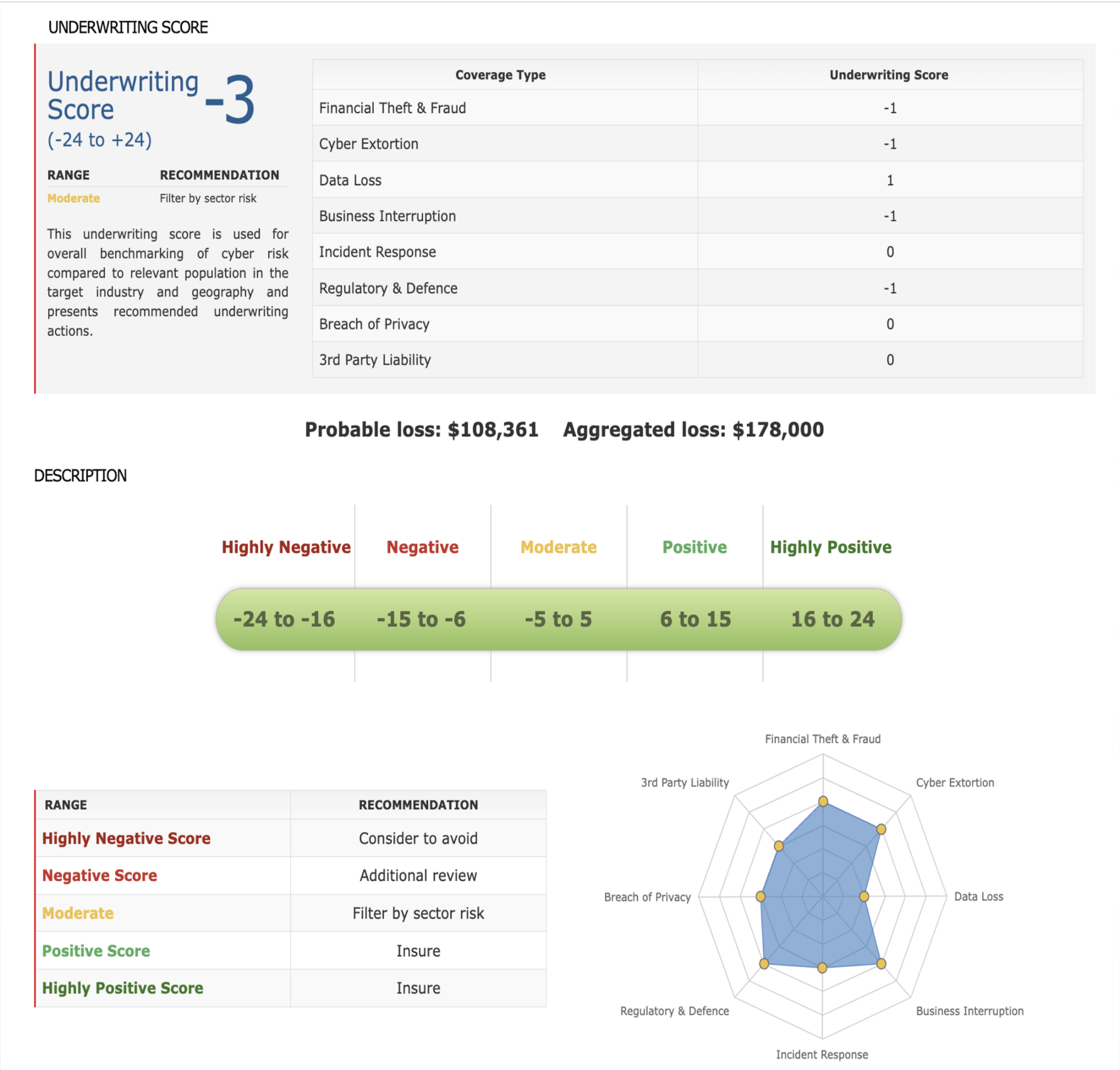
You can view the full list of security alerts here.

Detailed information

Type	Severity	Previous Value	Current Value
Count of Exposed Credentials	High	193	222

DEDICATED UNDERWRITING RECOMMENDATIONS

A dedicated Underwriting score to enable agile industry comparison and provide actionable insights.



UNDERWRITING SCORE

Underwriting Score -3
(-24 to +24)

RANGE	RECOMMENDATION
Moderate	Filter by sector risk

This underwriting score is used for overall benchmarking of cyber risk compared to relevant population in the target industry and geography and presents recommended underwriting actions.

Coverage Type	Underwriting Score
Financial Theft & Fraud	-1
Cyber Extortion	-1
Data Loss	1
Business Interruption	-1
Incident Response	0
Regulatory & Defence	-1
Breach of Privacy	0
3rd Party Liability	0

Probable loss: $108,361 **Aggregated loss: $178,000**

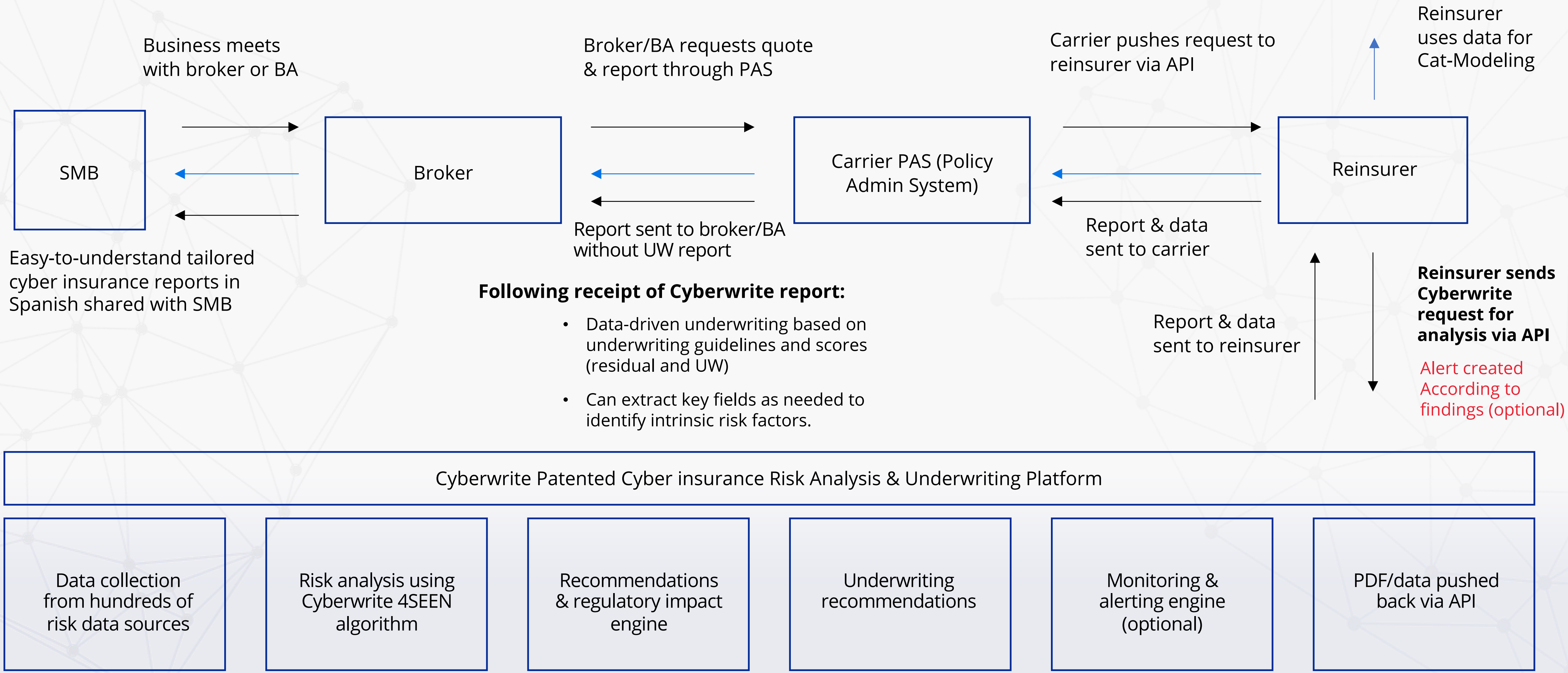
DESCRIPTION

Highly Negative	Negative	Moderate	Positive	Highly Positive
-24 to -16	-15 to -6	-5 to 5	6 to 15	16 to 24

RANGE	RECOMMENDATION
Highly Negative Score	Consider to avoid
Negative Score	Additional review
Moderate	Filter by sector risk
Positive Score	Insure
Highly Positive Score	Insure

Use Case

API BETWEEN CYBERWRITE, REINSURER , CARRIER , AGENTS AND SMBS



Business meets with broker or BA

Broker/BA requests quote & report through PAS

Carrier pushes request to reinsurer via API

Reinsurer uses data for Cat-Modeling

SMB

Broker

Carrier PAS (Policy Admin System)

Reinsurer

Easy-to-understand tailored cyber insurance reports in Spanish shared with SMB

Report sent to broker/BA without UW report

Report & data sent to carrier

Report & data sent to reinsurer

Reinsurer sends Cyberwrite request for analysis via API

Alert created According to findings (optional)

Following receipt of Cyberwrite report:

- Data-driven underwriting based on underwriting guidelines and scores (residual and UW)
- Can extract key fields as needed to identify intrinsic risk factors.

Cyberwrite Patented Cyber insurance Risk Analysis & Underwriting Platform

Data collection from hundreds of risk data sources

Risk analysis using Cyberwrite 4SEEN algorithm

Recommendations & regulatory impact engine

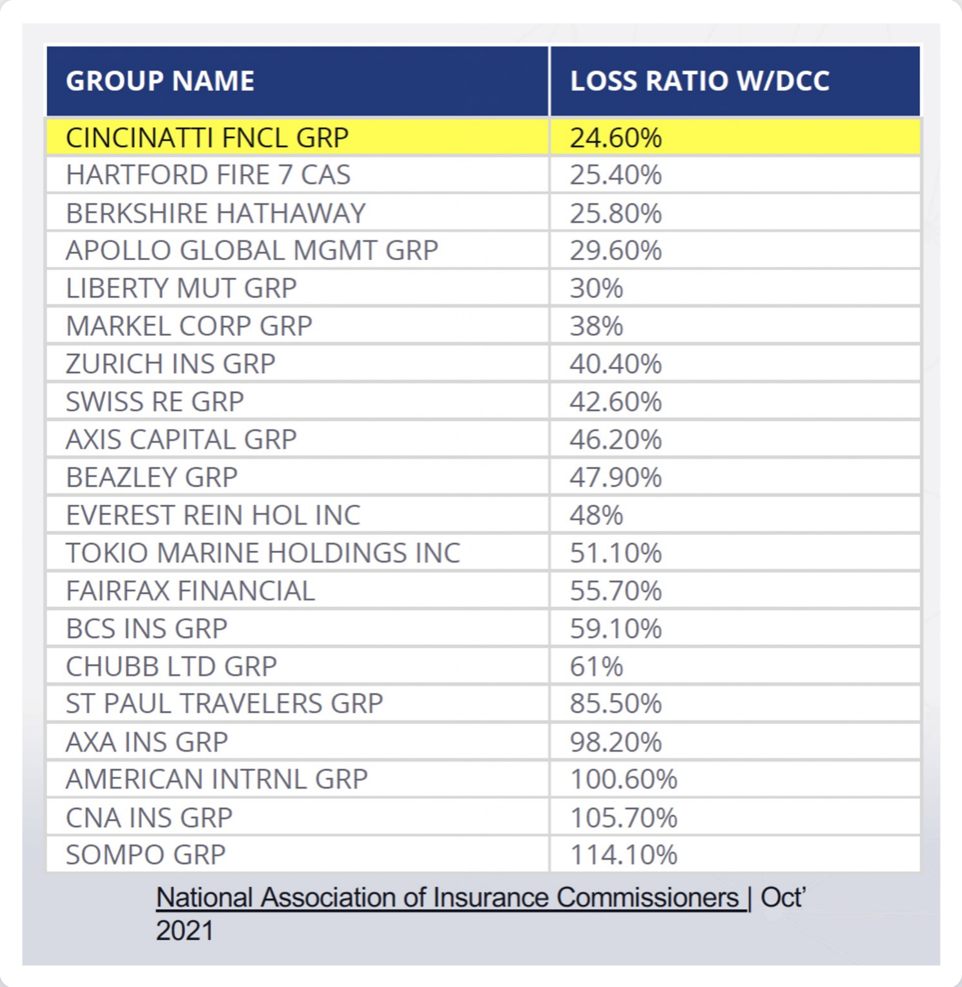
Underwriting recommendations

Monitoring & alerting engine (optional)

PDF/data pushed back via API

Underwriting

CYBERWRITE USERS EXPERIENCE LOWER LOSS-RATIOS



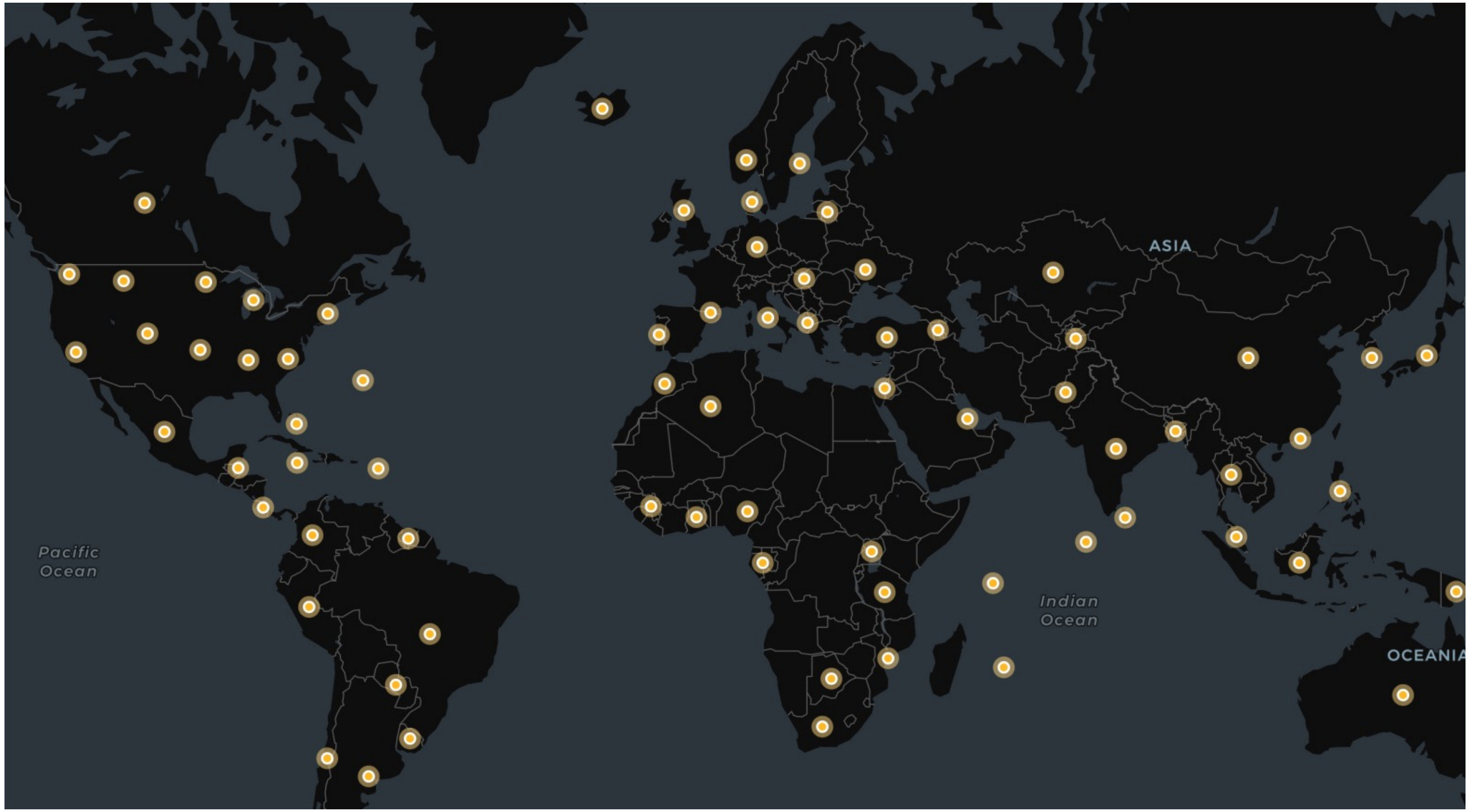
GROUP NAME	LOSS RATIO W/DCC
CINCINATTI FNCL GRP	24.60%
HARTFORD FIRE 7 CAS	25.40%
BERKSHIRE HATHAWAY	25.80%
APOLLO GLOBAL MGMT GRP	29.60%
LIBERTY MUT GRP	30%
MARKEL CORP GRP	38%
ZURICH INS GRP	40.40%
SWISS RE GRP	42.60%
AXIS CAPITAL GRP	46.20%
BEAZLEY GRP	47.90%
EVEREST REIN HOL INC	48%
TOKIO MARINE HOLDINGS INC	51.10%
FAIRFAX FINANCIAL	55.70%
BCS INS GRP	59.10%
CHUBB LTD GRP	61%
ST PAUL TRAVELERS GRP	85.50%
AXA INS GRP	98.20%
AMERICAN INTRNL GRP	100.60%
CNA INS GRP	105.70%
SOMPO GRP	114.10%

National Association of Insurance Commissioners | Oct'
2021

https://www.insurancejournal.com/app/uploads/2021/11/NAIC-Cyber_Insurance-Report-2020.pdf

GLOBAL SPREAD

Cyberwrite Provides Reports in Six Different Languages in over 40 countries



THE CYBERWRITE ADVANTAGE (1/2)

Lowers risk exposure and loss ratios for carriers

On Demand Real-Time Profiling

- Not limited to a database of pre-profiled companies.
- Can create a risk report for nearly any company worldwide.

Cyber Insurance Dedicated Platform

- Cyberwrite AI models adapt to specific cyber insurance policies for optimal, tailored results.
- Competitor products based on third-party risk management (TPRM), resulting in less effective scoring.

Easy-to-Understand

- Provides simple risk score, benchmarking, damage estimation, and other critical cyber data.
- Enables insurers to identify businesses with less risk, and insureds to prioritize and mitigate risks.

Financial Damage Predictions

- Provided by risk/coverage type
- Enables insurance professionals to demonstrate ROI of cyber insurance and SMBs to improve their cyber security and mitigate future damages and fines.

Recommendations & Regulatory Impact Analysis

- Identifies and demonstrates gaps in regulatory frameworks to enable insureds to mitigate present and future vulnerability.

Ongoing/Active Monitoring

- Offered throughout the policy lifecycle via a dedicated insured portal, providing ongoing awareness and enabling SMBs to address evolving risks.

THE CYBERWRITE ADVANTAGE (2/2)

Lowers risk exposure and loss ratios for carriers

Extensive, Proprietary Datasets

- Years of proprietary and extensive cyber insurance data, and R&D insights enables Cyberwrite to profile nearly any business at any time.
- Most competitors have data on a very limited number of companies and can't provide reports to SMBs in real-time.

Patented, Cyber Insurance AI (4SEEN®)

- First-of-its-kind cyber insurance AI risk analysis algorithms consistently show a correlation to lower-than-average loss ratios.
- 3" party risk management providers' scores do not correlate strongly to claims of cyber insurance.

Adaptive to New Risks

- Cyberwrite can continually implement new risk scenarios as risks evolve and has provided these services to blue-chip insurers
- Cyberwrite can realign ML classifiers for updated risk scenarios and data, differentiating it from competitors.

Dedicated aggregation & augmentation modules

- Provides unparalleled capabilities for insurance book analytics uncover accumulation points & prevent catastrophes.

RESTful APIs

- Uses API to streamline data into existing policy administration systems and other platforms.

REPORT GENERATION PROCESS

01	**Data Collection**	Draws on multiple external and internal data points for cyber risk analysis.
02	**Data Mapping**	AI and ML based mapping of classifiers for various damage types and insurance coverages specific to the insurance/cyber insurance industry.
03	**Industry Comparison**	Benchmarks risk profile to a growing subset of over 300K organizations and generates industry median score to indicate risk level.
04	**Weighting**	Assigns weights for each AI classifier and each damage type, based on the unique characteristics of each business.
05	**Scoring Damage Types**	Scores types of damage for each of the risk types / coverage types, such as financial theft & fraud, cyber extortion, data loss, business interruption, incident response, regulatory & defense, breach of privacy, and 3rd party liability.
06	**Risk Score & Impact**	Calculates inherent and residual risk scores and economic damage in case of a breach with quantification ranging from 1 to 100. Higher scores correlate to a lower probability of a cyber incident compared to industry peers.

Example success story

MAPFRE Utilizing Cyberwrite for SMB Underwriting and Security

MAPFRE

“With Cyberwrite, we are taking a leap forward in the evaluation, monitoring, and control of cyber risk, obtaining insights that are very useful for the teams to make data-driven underwriting decisions.”

Oscar Taboada Tomás

Head of Underwriting Europe & Head of Cyber at
MAPFRE RE COMPANIA DE REASEGUROS S.A.

“

Example success story

MUNICHRE’S HSB & CINFIN (SAAS + API INTEGRATION)

”

Munich RE®

1866
Hartford Steam Boiler

“Cyberwrite is a great partner to work with and they have a solid understanding of the cyber risks that all businesses face in today’s world. Cyberwrite helps us to quantify and manage our cyber risks across HSB’s portfolio.”

Steve McWilliams

Cyber Risk Services Manager @ HSB Munich Re

Cyberwrite

Thank You!

Contact us to schedule a demo:

✉ info@cyberwrite.com 🌐 www.cyberwrite.com