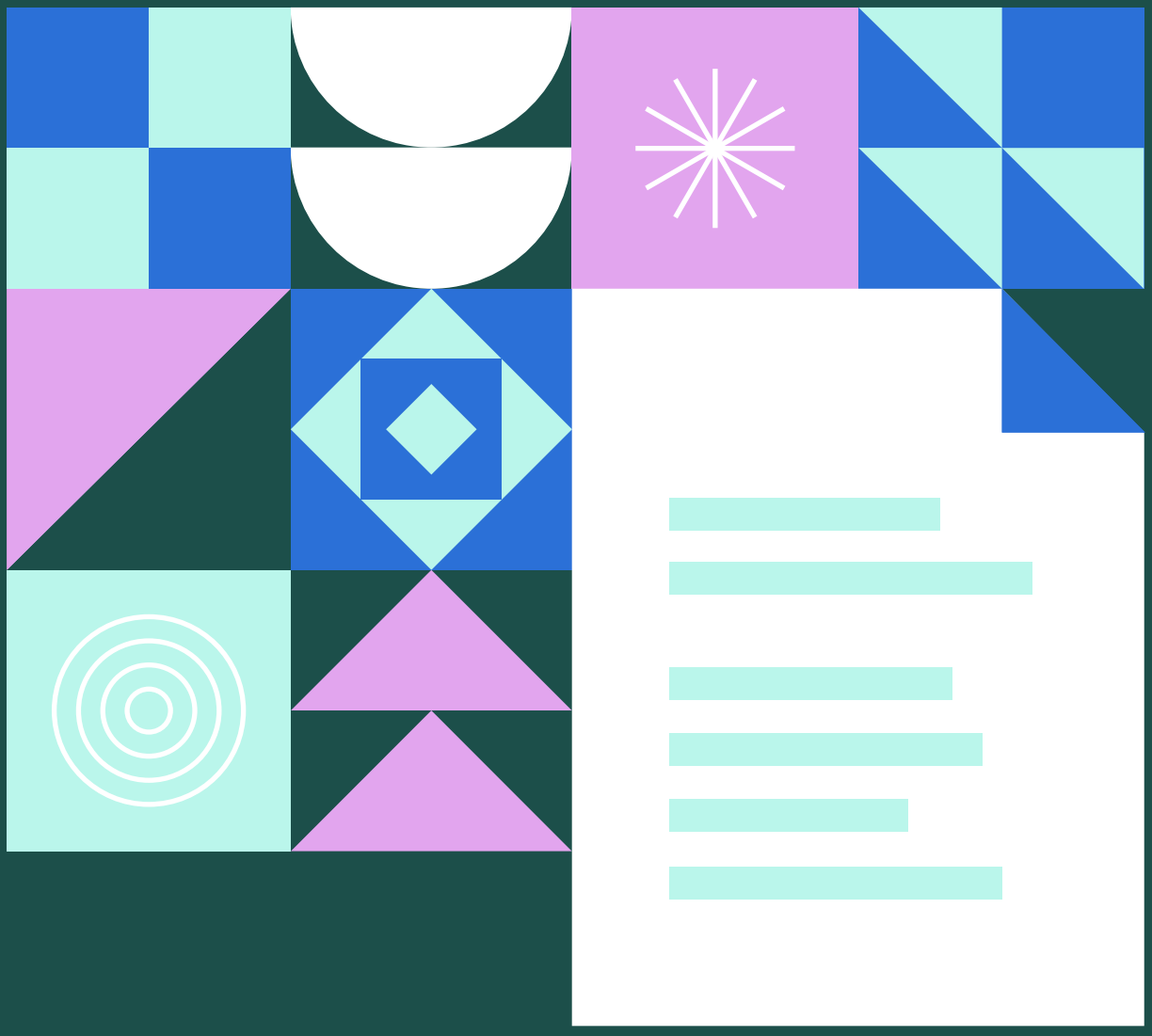
Coalition®

coalitioninc.com



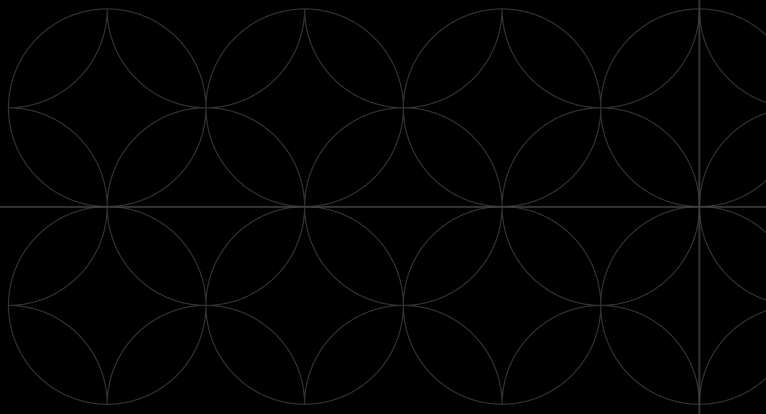
2022 Cyber Claims Report

Mid-year Update

Table of Contents

2022 Cyber Claims Report

Mid-year Update



Executive Summary

The cyber landscape is constantly evolving. To keep pace with the speed of cyber incidents and their accompanying claims, Coalition releases data semi-annually to give commercial insurance brokers, policyholders, and the industry a fresh perspective supported by data from our in-house claims team.

Coalition's 2022 Cyber Claims Report Mid-year Update is based on our dataset built from the 160,000 (and growing) businesses we protect. This report aims to help brokers educate their clients on how to reduce their cyber risk exposure, plus demonstrate why Active Insurance is a better model of protection for the fast-moving nature of cyber risks.

Key findings in this report show Coalition customers experienced significantly fewer claims in the first half of 2022, and they also resulted in less costly downtime.

However, this report also shows an increase in attacks targeting small- and mid-sized organizations with fewer resources to respond to attacks.

Our claims data on the top cyber incident trends also reinforces the need for continued vigilance from organizations of all sizes. Cyber criminals have created a profitable revenue model that is here to stay, and their number one attack vector continues to be phishing vulnerable humans.

Keep reading for more insights on the top cyber incident trends in 2022 from Coalition's claims data.

01 Overall cyber incidents are down

The surge in cyber crime in recent years highlights the need for businesses to have insurance coverage for digital risks. However, the first half of 2022 saw a slight decrease in both the severity and frequency of cyber claims among Coalition policyholders.

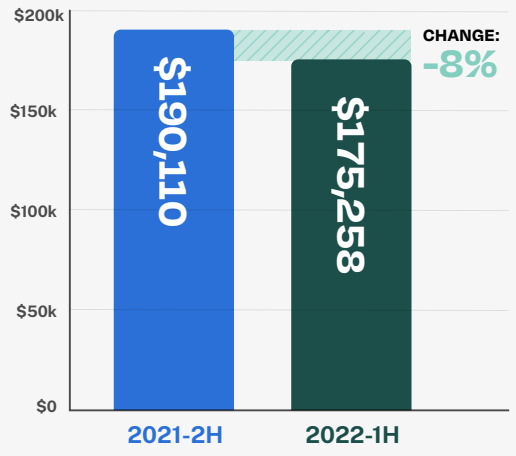
According to our data, policyholders experienced 50% fewer claims compared to the broader market,[1] with 45% of incidents resolved at no cost.[2]

Also notable in the data was how claims severity decreased by 8% for H1 2022 (compared to H2 2021) to an average loss of $175,258, and claims frequency decreased by 7% over the same period.

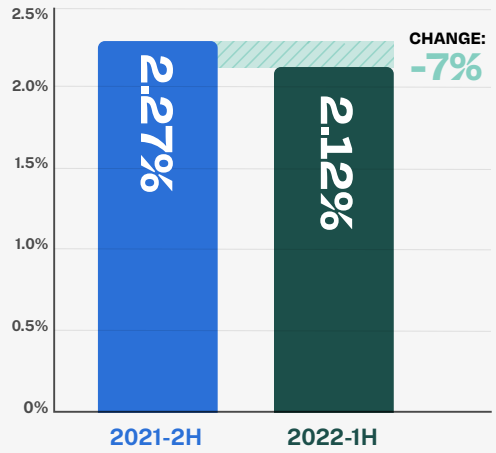
Manufacturing and industrial businesses related to the supply chain continue to top the charts as the most targeted industries. The data also shows a staggering 57% increase in claims frequency for nonprofit policyholders.

Coalition policyholders experienced fewer claims compared to the broader insurance market.

Severity of cyber claims among Coalition policyholders



Frequency of cyber claims among Coalition policyholders



02 Small businesses became bigger targets

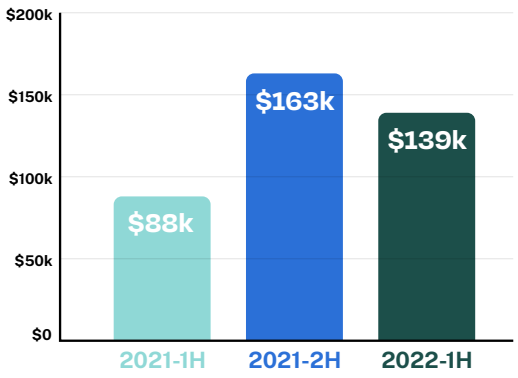
In 2021, we observed that small businesses with under $25M in revenue had become increasingly vulnerable to cyber incidents. Overall claims severity for this cohort of policyholders saw a drastic spike in H2 2021, rising 85% versus H1 2021 to $163,000.

While it may seem encouraging that 2022 has seen a 15% decrease in severity to $139,000 to date, the average claim cost remains significant for small businesses and is 58% higher than H1 2021 levels. Organizations of this size are especially vulnerable to threat actors as they often lack the resources to quickly respond to an attack.

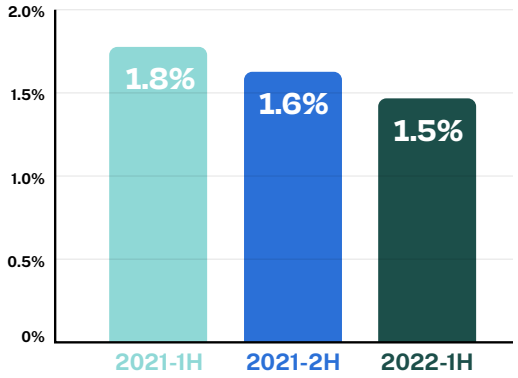
Cyber incidents have the power to put very small organizations out of business. This trend has also been observed by other key industry players, including Verizon's 2022 Data Breach and Investigations Report (DBIR), which included very small businesses (defined by 10 or fewer employees) for the first time.

The average cost of a claim for a small business owner was $139,000.

Severity of claims reported by Coalition policyholders



Frequency of claims reported by Coalition policyholders



03 Phishing triggers the majority of cyber incidents

Employees are typically the most exploitable aspect of any organization's security, making remote workforces more vulnerable to phishing. This is because supporting employees across different geographies and technologies makes it more difficult to validate communications and requests.

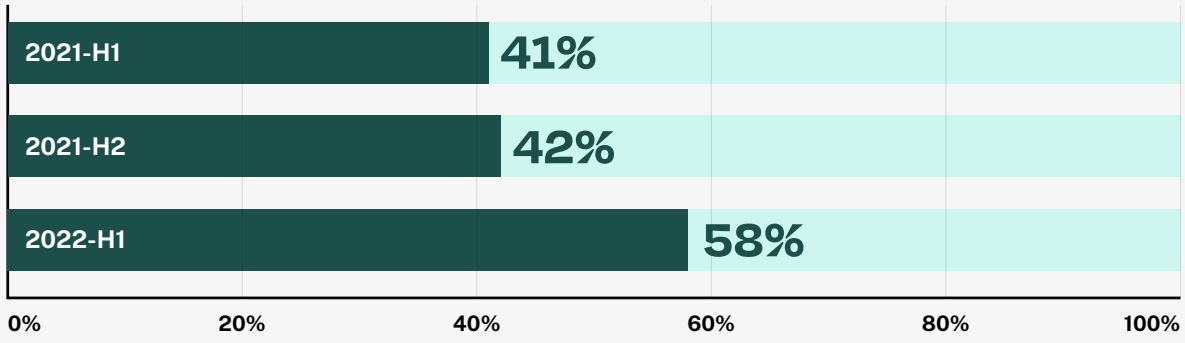
Year after year, phishing remains one of the most common attack vectors resulting in cyber insurance claims for Coalition policyholders.

In H1 2022, phishing accounted for 57.9% of reported claims[2]—a 32% increase from H2 2021.

For context, in H1 2021, email phishing was the initial attack vector for 41% of reported claims, and in H2 2021, this number rose slightly to 42%.

In H1 2022, phishing accounted for 58% of reported claims[2]—a 32% increase from H2 2021.

Percentage of claims with phishing as the primary attack vector



04 Ransomware declines as demands go unpaid

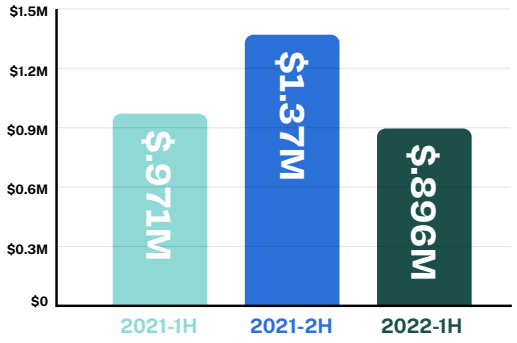
As ransomware incidents exploded in 2020, ransom demands and frequency continued to increase while claims severity started to plateau. Among Coalition policyholders, in H1 2022 there has been a slight decrease in both ransomware frequency and severity versus H2 2021, but the biggest shift is the decrease in both ransom demands and payment.

Ransomware demands decreased from $1.37M in H2 2021 to $896,000 in H1 2022. **Of the incidents that ultimately resulted in a payment, Coalition negotiated the payment down to an average of 20% of the initial demand.**

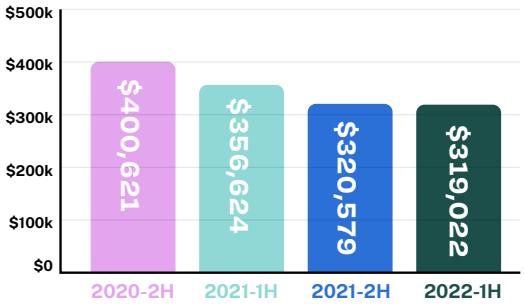
Coalition has found that companies that have implemented security controls such as offline data backups may refuse to pay the ransom and restore operations through other means. Coveware reported more large organizations are refusing to consider ransom negotiations. They also observed a drop in the median ransom payment, which decreased 51% to $36,360 in Q2 2022.[3]

Additionally, Verizon's 2022 DBIR reviewed ransom incidents and found that 60% of attacks didn't result in payment, leading them to liken ransomware to a lottery.

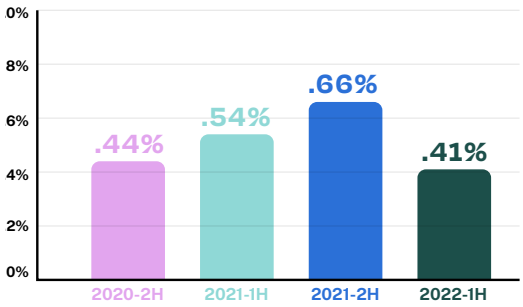
Average ransom demand made against Coalition policyholders



Severity of ransomware claims made by Coalition policyholders



Frequency of ransomware claims made by Coalition policyholders



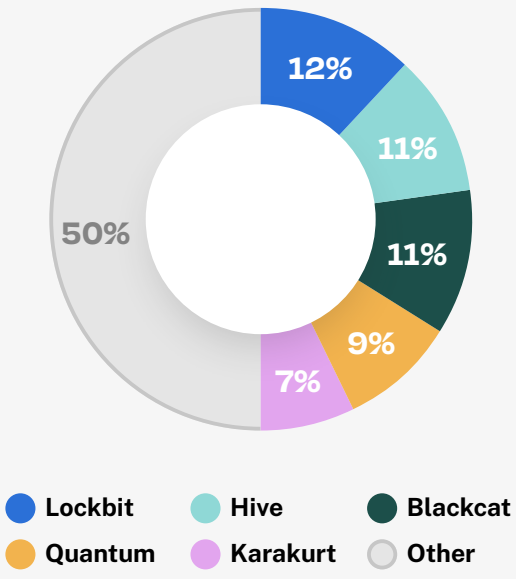
05 Cyber gangs built a thriving business

Ransomware gangs are holding organizations of all sizes hostage in exchange for exorbitant fees. Over the last three years, cyber attacks have evolved into a viable criminal business model with threat actor groups such as Conti, Lockbit, and Hive continuing to make headlines.

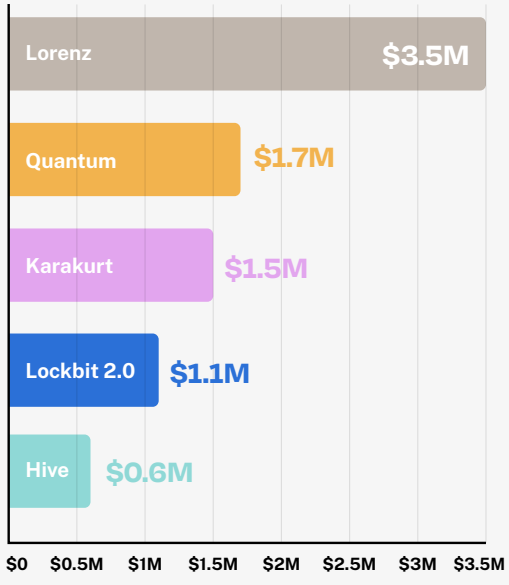
While it's encouraging that more businesses are able to recover without paying the ransom, we expect ransomware gangs to respond by evolving their business model that has proved to be so lucrative.

Year over year, Coalition sees an evolving set of leading ransomware variants. For 2022, many of the top ransomware variants can be directly associated with or leased from the Conti ransomware gang, such as Karakurt — a known data extortion arm of Conti.

Top ransomware variants by percentage of claims reported



Top ransomware variants by average ransom demand in 1H 2022

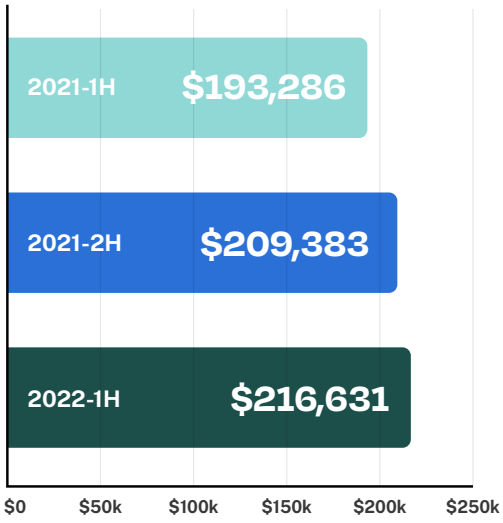


06 Funds Transfer Fraud (FTF) claims hold steady

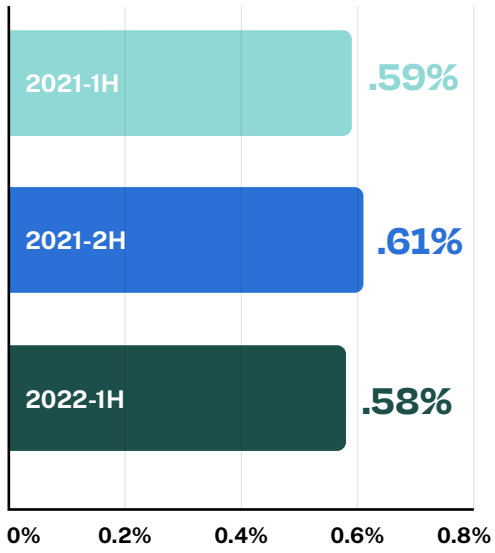
The single weakest link in an organization's security fence is its employees. With more businesses continuing to allow remote or hybrid work models, employees may sometimes let their guard down and fall victim to phishing emails. As observed by Coalition's Claims team, phishing through business email compromise (BEC) often leads to funds transfer fraud (FTF) events, a type of attack where threat actors redirect or change payment information to steal funds.

FTF events remained relatively consistent. The frequency of incidents decreased by only a few basis points, dropping from 0.61% in H2 2021 to 0.58% in H1 2022. However, FTF severity has increased by 3% in the same period, continuing the 3-year trend of increasing FTF claims costs.

Severity of FTF claims made by Coalition policyholders



Frequency of FTF claims made by Coalition policyholders



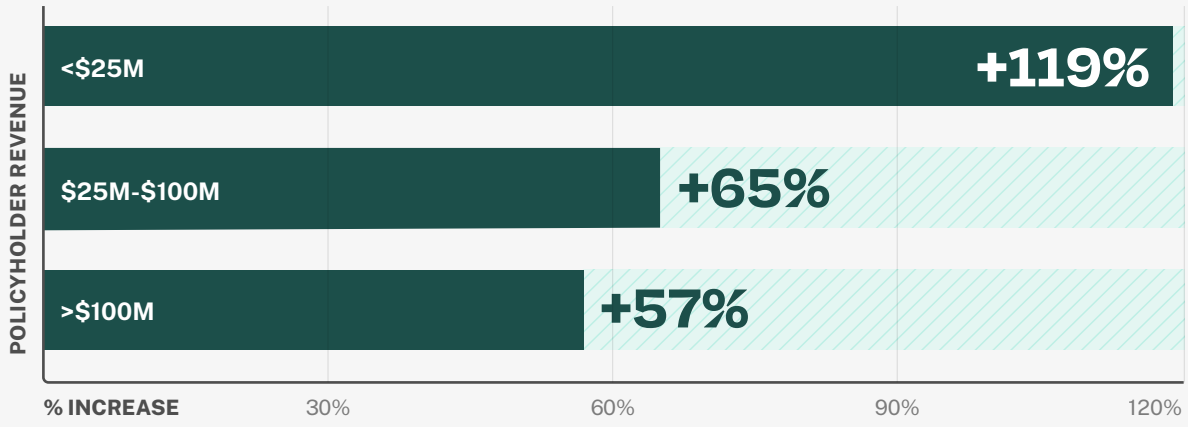
07 The vulnerability that persists: Microsoft Exchange

In 2021, Microsoft disclosed an exploitable condition (ProxyLogon) that was found in publicly accessible Microsoft Exchange servers. During this time, approximately 1,000 Coalition policyholders were affected. We were able to notify and remediate the vulnerability for 98% of impacted policyholders within a week of the disclosure.

In August of 2021, another vulnerability related to on-premises Exchange (ProxyShell) was discovered. Coalition developed a dedicated scanning module to handle Exchange events, which can report on the version of Exchange an organization is running. Using our Active Risk Platform, we continue to monitor externally visible data and notify our policyholders if they have exposed Exchange vulnerabilities.

Based on our data set, since the discovery of this vulnerability, smaller organizations with on-premise Microsoft Exchange were 119% more likely to incur a claim than those using Exchange Online.

Microsoft Exchange-related claims by policyholder revenue band



Conclusion

Continued vigilance with an active approach

The shifting nature of digital threats and the rapid adaptation of threat actors' techniques support the need for a continued, active approach to managing risk.

Coalition is the world's first Active Insurance company. By combining the power of technology and insurance, we help organizations identify, mitigate, and respond to digital risks[4]. Thanks to our active monitoring and alerting capabilities — and our in-house incident response and claims teams — our policyholders experience fewer attacks and lower claims costs.

As part of our partnership, we believe in empowering brokers to build their knowledge and expertise of the changing cyber threat landscape, enabling them to become trusted advisors to their clients.

We hope this report, along with consultative tools such as personalized Cyber Risk Assessments, will help you advise your clients to take an active role in managing their risks as part of our commitment to providing **security for all**.

REFERENCES

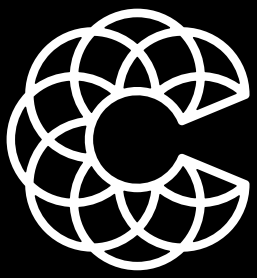
1. Market data is reported by US insurers to the National Association of Insurance Commissioners (NAIC). Coalition compares claims frequency from our claims data to the NAIC 2021 report on an earned policy basis for each calendar year.

2. Data is based on the determination of root cause as reported by Coalition's Incident Response, Inc., a forensic vendor engaged by certain Coalition insureds.

3. Data reported in Coveware's July 28, 2022 Quarterly Report "Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022"

4. In the United States, insurance products are offered by Coalition Insurance Solutions, Inc. ("Coalition Insurance Solutions"), a licensed insurance producer with its principal place of business in San Francisco, California (Cal. license # 0L76155) acting on behalf of Swiss Re Corporate Solutions America Insurance Corporation. Because many of our clients need access to surplus lines insurers, Coalition Insurance Solutions is also a surplus lines broker. See licenses at coalitioninc.com/licenses. Insurance products offered through Coalition Insurance Solutions may not be available in all states and surplus lines insurers are generally not licensed in a particular state. In Canada, insurance products are offered by Coalition Insurance Solutions Canada Inc. ("CIS Canada"), a licensed insurance producer with its principle place of business in Vancouver, British Columbia Canada, a licensed insurance producer in all Canadian provinces except Quebec. See licenses at coalitioninc.com/en-ca/licenses. CIS Canada acts on behalf of insurers: Arch Insurance Canada Ltd. and Westport Insurance Corporation, respectively.

   Both Coalition Insurance Solutions and CIS Canada may receive compensation from an insurer or other intermediary in connection with the sale of insurance to a policyholder. All decisions regarding any insurance products, including approval for coverage, premium, commissions and fees, will be made solely by the insurer underwriting the insurance under the insurer's then-current criteria. All insurance products are governed by the terms, conditions, limitations and exclusions set forth in the applicable insurance policy. Please see a copy of your policy for the full terms, conditions and exclusions. Any information in this advertising material does not in any way alter, supplement, or amend the terms, conditions, limitations or exclusions of the applicable insurance policy and is intended only as a brief summary of the insurance products available. Policy obligations are the sole responsibility of the issuing insurance carrier.



Coalition®

coalitioninc.com

55 2ND STREET, SUITE 2500
SAN FRANCISCO, CA 94105

Coalition, Inc.
@SolveCyberRisk
Coalition, Inc.
help@coalitioninc.com