2023 Canada Cyber Market Conditions Outlook Report

Gallagher

Insurance | Risk Management | Consulting

January 2023

THE CYBER INSURANCE MARKET BEGINS TO STABILIZE

By: Dan Lewis
SVP National Management Liability Practice, CA

After three years of hardening conditions, the cyber insurance market has finally begun to show signs of stabilization. From a premium perspective, cyber insurance buyers are seeing smaller rate increases and, in some cases, even flat renewals.

There are, however, clear signs that we will not be reverting to the soft market conditions from a few years ago. First, the offered products cover less with new restrictive policy wording imposed by several carriers in 2023. Secondly, the strict underwriting control requirements mandated last year will persist while the demand for capacity appears to continue to outpace supply. Finally, there is a growing concern among cyber insurance markets around systemic cyber risk, where the focus remains on quantifying a potentially catastrophic cyber event and estimating the probability of one occurring. This underlying concern will likely persist through 2023 and work to support the current conditions that will maintain the tenants of a challenging cyber insurance marketplace.

WHAT WE SAW IN 2022

In the first quarter of 2022, the FBI released its 2021 Internet Crime Report detailing all 2021 losses. The FBI reported potential ransomware losses exceeding $6.9 billion USD. Also, in the report were the most commonly reported incidents: business e-mail compromise ("BEC"), and the criminal use of cryptocurrency. Of note, while ransomware made headlines, the FBI reported that BEC schemes resulted in 19,954 complaints with an adjusted loss of nearly $2.4 billion USD.

In February of 2022, we saw the conflict between Ukraine and Russia erupt, which stoked fears of a larger global cyber conflict that could potentially impact organizations exposed to collateral damage, if not targeted directly by Russia. Fortunately, those concerns never did manifest, and the cyber market breathed a sigh of relief. As 2022 progressed, the frequency and severity of ransomware attacks leveled off and, by some estimates, trended downward. According to one report,[1] ransomware attacks in the first nine months of 2022 declined by 31% year-over-year—a considerable factor in 2022s slowing the dramatic upward climb in rates from the year before.

LAW ENFORCEMENT ACTION AGAINST CYBERCRIMINALS USING RANSOMWARE

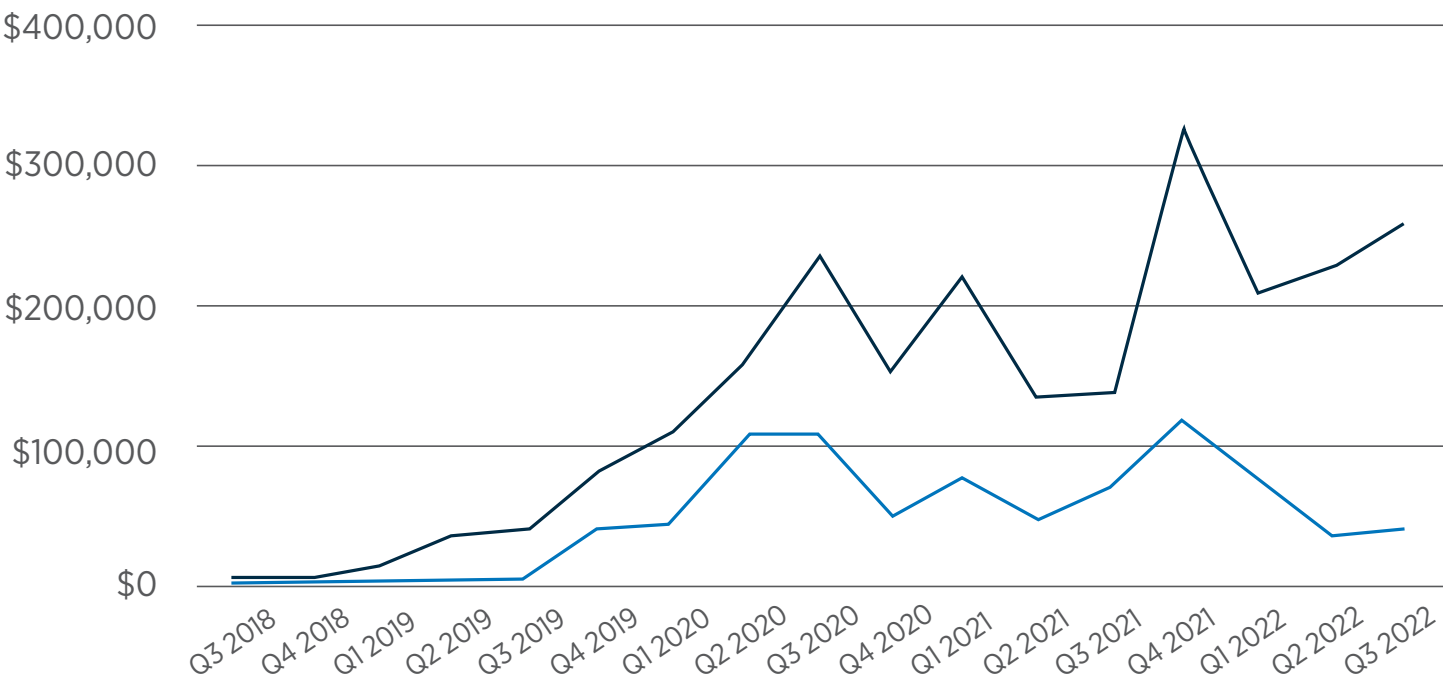
In May 2021 and again in early 2022, the Cyber Centre observed a decrease of ransomware incidents against Canadians. We assess this was likely a result of threat actors seeking to avoid law enforcement attention directly following international action.

While law enforcement action almost certainly disrupts cybercriminal operations, we judge that these disruptions rarely have an enduring effect on the ransomware environment. Weeks after Russia's arrest of 14 individuals associated with a prominent ransomware gang in early 2022, cybersecurity researchers observed the ransomware group back up in operation.

RANSOMWARE-AS-A-SERVICE HAS MADE RANSOMWARE MORE ACCESSIBLE AND PROFITABLE

Much of the ransomware affecting Canadians is very likely owned by ransomware-as-a-service (RaaS) cybercrime groups. These groups create and maintain ransomware variants and sell access to other cybercriminals who deploy the ransomware against a victim. Ransomware-as-a-service groups request upfront payment, subscription fees, a cut of profits, or all three in exchange for access to their ransomware, lowering the barrier to entry for criminals.

Average and Median Ransom Payment in Q3 2022 (USD)[2]



In Canada, claims statistics are inherently difficult to obtain, as many breaches are not clearly reported, or the dollars are not disclosed. We rely on a series of studies for Canada polling those that have suffered breaches, and a few highlights are noted below[3]:

- Twenty-nine percent (29%) of organizations experienced a breach last year; 82% reported that their organization had a cyber IRP (CIRA study)
- Canadian anti-fraud centre advised that there have been over 150,000 reports of cyber fraud with over $600 million CAD stolen since Jan 2021
- 2022 Ponemon Cost of a Data Breach[4]
- $6.35 million CAD average cost
- Average ransomware amount $228,000 USD, up 8% from Q1 to Q2 2022
- Eighty-six percent (86%) of cases threaten to leak exfiltrated data, with average organization downtime at 24 days

MARKET HEALTH/RATINGS

We noted some long-awaited good news for the market in the Fitch Ratings report that was released in June. Specifically, Fitch noted robust growth in the cyber insurance market and improved cyber loss ratios amongst carriers.

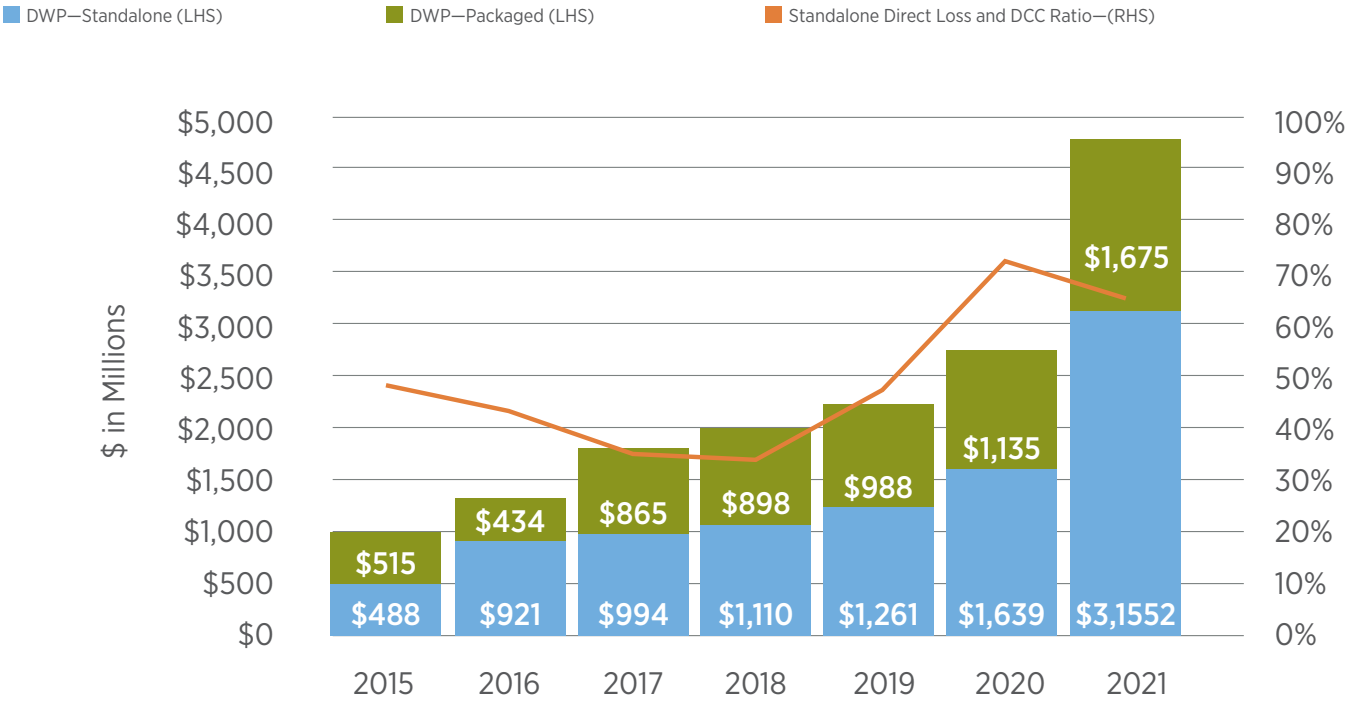
> A sharp increase in 2020 cyber loss ratios promoted substantially higher prices and rapid premium growth in 2021 that exceeded incurred losses, leading to surprising improvement in the cyber direct loss ratios versus the previous year."

Some key findings in the Fitch report reflected the fact that cyber underwriting profits improved while there was a noted increase in cyber insurance adoption amongst insurance buyers:

- Losses increased by over 300% since 2018. Still, 2021 premium growth exceeded the change in incurred losses and the standalone cyber loss ratio improved to 65% from 72% a year earlier.
- Fitch estimates that standalone and packaged cyber statutory direct written premiums increased by 74% in 2021 to nearly $5 billion USD compared with 9% growth for the P/C industry overall.
- Standalone cyber coverage increased by 92% in 2021.

P/C Industry Aggregate Standalone and Packaged Cyber Risk (USD)

Standalone Cyber Coverage loss Ratios improved to 65% from 72% in 2020



Standalone Direct loss and DCC ratios: 2015–48%, 2016–43%, 2017–35%, 2018–34%, 2019–47%, 2020–72%, 2021E–65%.

Statutory Cybersecurity and Identity Theft Coverage Supplement Data. DCC—Defense and cost containment incurred.

Source: Fitch Ratings, S&P Global Market Intelligence.

Regulators made their voices heard in 2022. According to the SEC's Statement on Proposal for Mandatory Cybersecurity Disclosure issued on March 9, 2022, all publicly traded companies must adhere to two mandates, among other requirements.

- **Mandatory cybersecurity incident disclosure.** Material incidents must be reported on an 8-K form within four business days of the incident. Organizations would also be required to provide periodic updates about previous incidents. In addition, they would be required to report when "a series of previously undisclosed, individually immaterial cybersecurity events has become material in the aggregate."
- **Required disclosures of company policies to manage cyber risks.** Annual reports would have to outline a firm's policies for identifying and managing cyber risks and document whether any member of its board of directors has expertise in cybersecurity.

Canadian securities laws currently do not impose any cybersecurity-specific disclosure requirements on reporting issuers, but the Canadian Securities Administrators have published guidance outlining their expectations regarding reporting issuers' disclosures in respect of material cybersecurity incidents and risks, and related mitigation strategies. However, if a Canadian company is traded on a US exchange, then the new SEC requirements will apply.

CLAIMS IN CANADA

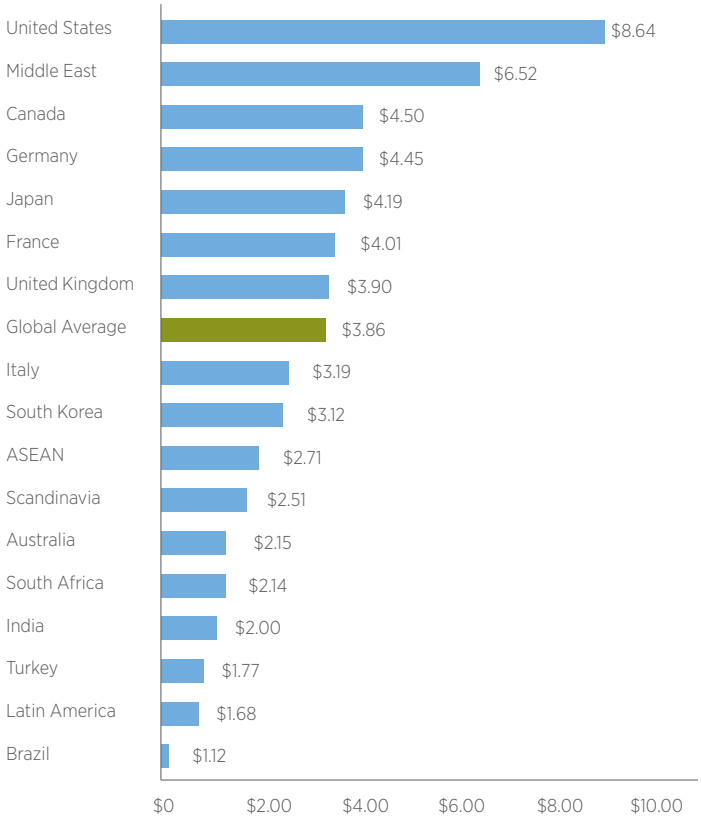
Privacy class action lawsuits in Ontario made headlines in 2022. A trio of lawsuits related to three high-profile claims in Canada (Equifax, Transunion and Marriott) argued the tort of intrusion upon seclusion and failed at both the lower court and the Ontario court of appeal. This is potentially precedent-setting, and would make it difficult for similar claims to succeed, when attempting to use 'intrusion upon seclusion' as the main cause of action. Stay tuned, as the plaintiffs may appeal to the Supreme Court of Canada.

In other news, the Empire Group (parent to grocery chains Sobeys and Safeway) disclosed in December 2022 that they would see a $25 million CAD hit to their earnings as a result of a 'cyber incident'. This amount was net of insurance recoveries.

In June 2022, Quebec courts approved a $200 million CAD class action settlement in the Desjardins case. In 2019, Desjardins discovered that a rogue employee had siphoned the personal information of up to 10 million Desjardins clients over a two-year period. This settlement is the largest in the Canadian Financial Services sector to date.

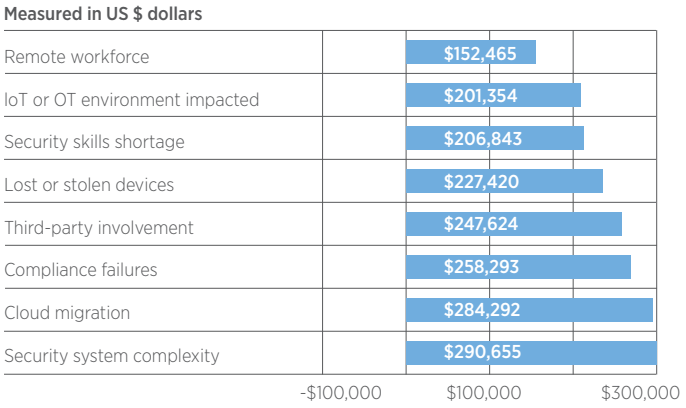
There were many other claims in Canada during the year, including manufacturers, education institutions, municipalities, food processors, unions, IT firms, nonprofits and retailers.

A comprehensive summary of recent losses related to cyber incidents was summarized in the Ponemon/IBM Security 2022 Cost of a Data Breach Report. The report again highlights Canada as one of the most expensive countries in the world to remediate a breach (in USD).

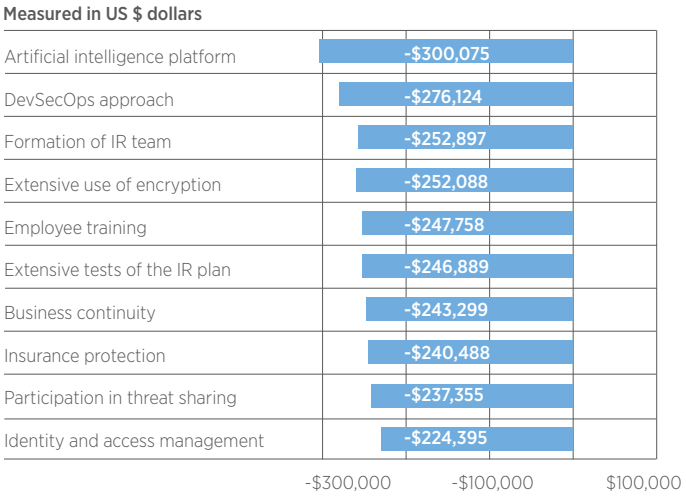


The Ponemon study also highlights several factors that could mitigate the cost of a data breach and others that may amplify them. Underwriters have continued to monitor these and other control factors, and remain focused on them in assessing their willingness to write policies for prospective insureds.

Key Cost Amplifiers



Key Cost Mitigators



What We Are Watching: Key Players That Will Shape the 2023 Market

We see the 2023 cyber marketplace reaching a level of maturity that we had not seen previously. A general understanding of expected cybersecurity controls has been established, and that expectation will be reinforced in 2023. After working through two or three policy renewal cycles in the hardening market, carriers have gained a greater comfort level in the risks they prefer to write moving forward. Several key players in the marketplace ecosystem will play crucial roles this year as this market continues to mature and grow. Their actions will profoundly impact the landscape that the cyber insurance buyer will ultimately need to navigate.

In Canada, price increases have begun to attract new capital. At least three new markets announced their intention to enter the market in 2022, so their impact may start to materialize in 2023.

Underwriters: Underwriters remain laser-focused on several controls, including multifactor authentication, endpoint detection and response, privileged access management, employee training, incident response planning along with other key cybersecurity controls. The application process, however, is still viewed as widely inefficient, time-consuming and prone to errors and miscommunication between underwriters, insureds and brokers. As a result, there will be an increased effort to streamline the process. This may be accomplished, at least in part, via an agreed upon third-party vendor solution that validates key controls are in place to a reasonable degree before underwriting decisions are made. We also expect some of the markets to modify policy wording to address concerns surrounding systemic cyber risk. This will include a focus on constricting coverage where multiple losses may result from a cyber-warfare event, losses stemming from a key player in the IT supply chain, or other attacks on critical infrastructure that lead to wide-ranging cyber losses.

Reinsurers: The reinsurance community has taken center stage on the important topic of capacity as it is viewed as imperative to the growth of the cyber insurance market. It is widely believed that it may come from both reinsurers and key capital markets via insurance-linked securities. However, before any meaningful progress can be made, there will be a need for improvements in cyber catastrophe modeling tools. Unlike those used for property insurance, cyber models do not have the luxury of analyzing multiple billion-dollar losses over a significant time frame, are challenged by a quickly shifting peril as the threat landscape evolves, and are using recently developed systems and software whose functionality and capabilities will likely have room for improvement.

Cyber Risk Management Vendors: We will see a continued trend of convergence of cybersecurity vendors with the insurance carrier and brokerage community. This may be accomplished through both strategic partnerships and acquisitions. The focus will be on leveraging key vendors to improve cyber loss quantification from both a single insured and a large number of insureds stemming from a wider systemic type of cyber loss event. In addition, cybersecurity vendors will have a continued and growing role in helping underwriters assess the risks of applicants and to provide ongoing cyber risk services for insureds throughout their policy terms.

Canadian Government: Canada's new federal privacy bill, Bill C-27, was tabled in June 2022. It should eventually replace the PIPEDA (Personal Information Protection and Electronic Documents Act) and amalgamate two other Acts. If enacted, it would apply to all private sector organizations in Canada. The legislation could impose significant fines and penalties on organizations who fail to protect personal information, similar to the EU's GDPR.

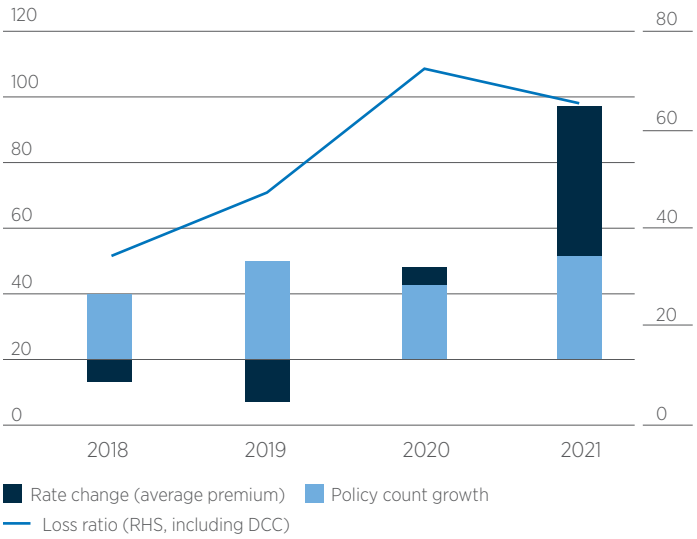
Looking Ahead

There is a growing consensus that the cyber insurance market is poised to grow exponentially in the near and far term. According to one estimate,[5] cyber insurance premiums reached $10 billion USD in 2021 and are projected to grow 20% year-over-year until 2025. That premium level, coupled with an estimated annual global cyber loss estimate of $945 billion USD,[6] leaves a vast majority of predicted cyber losses uninsured.

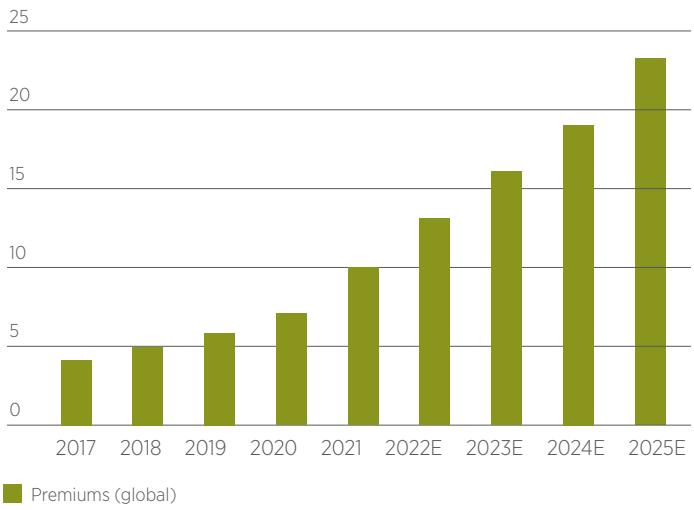
The Canadian cyber insurance marketplace is a small proportion of the global figure. Best estimates place the premium volume in Canada at roughly $400 million CAD, but losses are still exceeding that, keeping loss ratios (losses paid divided by premium collected) north of 100%. However, the loss ratio has fallen significantly, as more companies purchase the coverage, internal controls improve and terms/conditions/pricing continue to be tight. The market continues to grow at a rapid pace, and we expect Canadian growth to exceed the 20% figure noted above for the foreseeable future. The adoption of cyber insurance began sooner in the US than in Canada, and the majority of organizations still do not have proper insurance in place, but that is changing.

This reality will play against an evolving threat landscape with a looming concern of a future catastrophic cyber event. The market will certainly expand, but will do so carefully with dynamic cyber insurance policy terms and creative efforts for capacity expansion. Underwriters will partner with vendors from the cybersecurity and compliance arenas. In summary, we see the potential for significant growth in the cyber insurance market in 2023 and in the years to follow. As the cyber insurance marketplace continues to mature, it will follow a path to form a more cohesive alliance with both cybersecurity and government sectors as cyber threats evolve.

Left: US standalone loss ratio, and rate and exposure growth



Right: Global cyber insurance premiums, USD bn, Swiss Re estimates



Source: National Association of Insurance Commissioners, S&P Global, Swiss Re Institute calculations

Sources:

[1] SonicWall: Ransomware down this year, but there's a catch • The Register

[2] Uber Verdict Raises New Risks for Ransom Payments | Coveware

[3] 2022 CIRA Cybersecurity Survey

[4] 2022 Ponemon Cost of a Data Breach

[5] Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks, Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks | U.S. GAO

[6] Swiss Re Institute Cyber insurance: strengthening resilience for the digital transformation McAfee. op. cit. from Swiss Re Institute Cyber insurance: strengthening resilience for the digital transformation