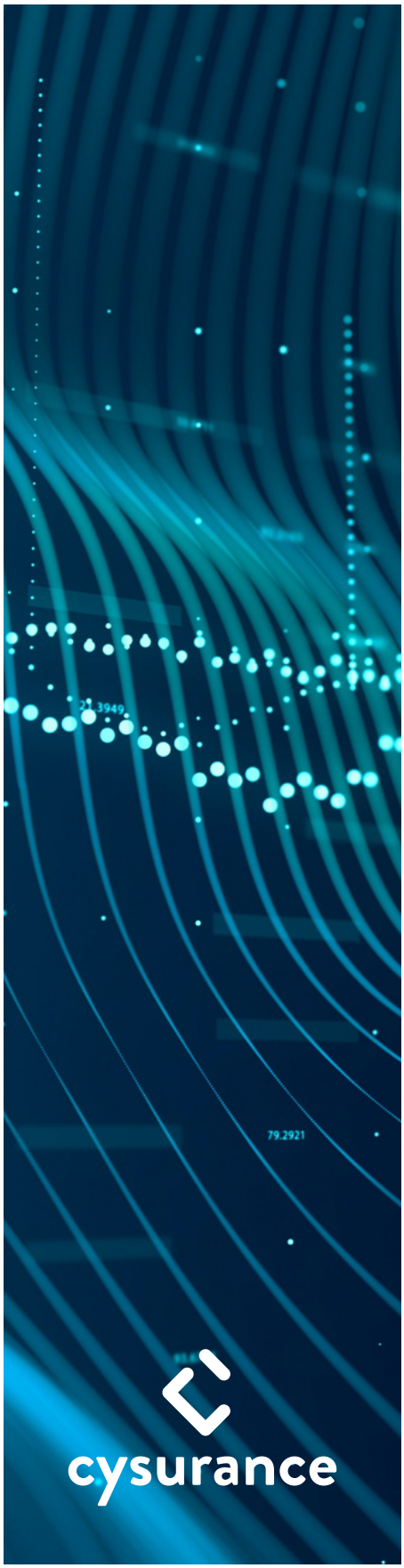
cysurance
e-book

CYSURANCE AS A SERVICE (CAAS)

Introducing a new layer of service protection for your customers

CYSURANCE AS A SERVICE: (CAAS)

Introduction



If 2020 has taught us anything, it's that unexpected events can have severe consequences. Now, more than ever, businesses need to plan for contingencies, including (*for the first time for many*) online assets and activities.

However, **COVID-19** introduced a new danger, not only to humanity but to the cyber risk landscape, resulting in unprecedented stress on network resources with workforces suddenly operating almost entirely remotely. Cybercriminals have taken advantage – ***impacting many businesses that were already in the challenging position of facing possible bankruptcy.***

Let's be honest – the insurance industry has not traditionally embraced innovation and for a business whose products are inherently complex, that position is difficult to defend in today's modern world, let alone during a global pandemic.

At **Cysurance**, we've listened to the market and leaned on our background in ***risk intelligence, cybersecurity, information management and policy expertise*** to develop a simple, technology-enabled platform that offers all the coverages a growing business needs for one low price.

Cysurance also leverages existing network products and services to help your clients implement an innovative cyber risk management strategy that improves claim outcomes and at the same time increases confidence in your managed services.

Increased confidence in your services can translate into more business opportunities, which could in turn translate into business growth.

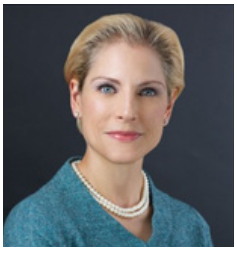
I see that as a win. **Especially in 2020!**

Welcome to a new way of doing business.

Welcome to **Cysurance** as a Service.

Kirsten Bay

Co Founder/CEO
Cysurance



CYSURANCE AS A SERVICE: (CAAS)

The insurance industry has not traditionally embraced innovation. For a business whose products are inherently complex, that position is difficult to defend in today's modern world.

It is especially true in the one line of insurance that is both increasingly critical for growing businesses and would seemingly depend on coverage clarity and adoption of new technology – cyber insurance. But cyber insurers are evolving to respond to emerging risks and changing market dynamics, and new insurtech platforms promise fit-for-purpose coverages and better claim outcomes, all delivered in a frictionless, online user experience.

The first step in this evolution has been the recognition that, in today's modern world, cyber risk is a unique and systemic exposure that requires dedicated limits, coverages and services. According to Accenture's 2019 Ninth Annual Cost of Cyber-crime Study¸ security breaches increased 67% in the last five years.

The New York Times reported the number of ransomware attacks increased 41% from 2018 to 2019, and Cybersecurity Ventures estimates that by 2021 businesses will suffer a ransom-ware attack every 11 seconds and cyberattacks will cost $6 trillion annually.

The FBI has seen the number of business email compromise reports grow from under 1,500 in 2014 to 23,775 in 2019, with corres-ponding financial losses growing from $60.3 million to $1.7 billion. Aqua Security says attacks on cloud servers have increased 250% from 2019 to 2020, with the majority deploying crypto-mining malware on victims' servers.

Complicating matters further, the FBI reports that as of June, digital crime had increased 75% since the beginning of the COVID-19 outbreak.

70% of respondents to a recent Ponemon survey expect remote workforces could increase the cost of a data breach. This latter stat highlights the role human error also plays in cyber risk, with email security company Tessian noting 54% of employees find workarounds when security policies prevent them from completing tasks. Additionally, Tessian notes data egress over email, USB and cloud devices has grown 80% since the pandemic's onset, with over 50% of that data marked as "classified".

On top of these threats, digital assets can be compro-mised by power outages and system failures. Nation-state and organized crime threat actors are growing bolder in their efforts. Hacktivists continue to push geopolitical and social agendas by attacking organi-zations' networks and insider threats have tripled between 2016 to 2019 according to the Ponemon
Institute.

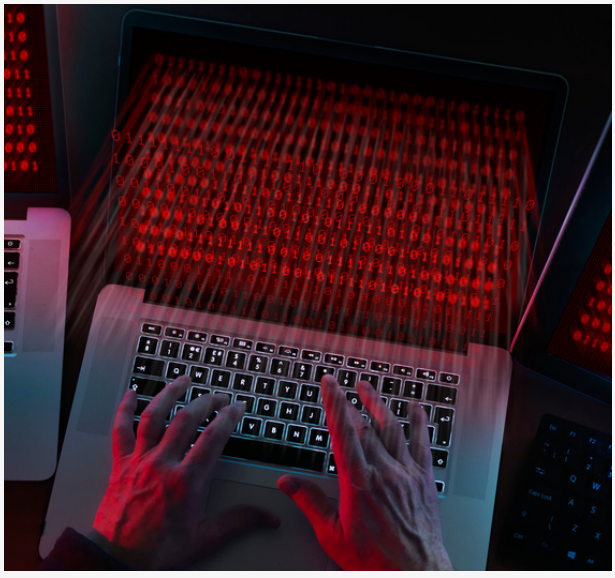
Cyber risks are also highly interconnected. An attack against a supplier, vendor or other service provider can have a severe impact on a company even if its own net-work security isn't comp-romised. The ransomware attack targeting the city of Baltimore in 2019 only demanded $76,000 worth of Bitcoin but cost the city an esti-mated $18 million by impacting vaccine production, ATM's, airports, hospitals and more. The infamous 2013 Target hack began with hackers gaining login credentials to the superstore's HVAC vendor, which had access rights to its network to remotely monitor energy cons-umption and store temperatures. The rapid growth of the IoT market, smart cities and smart factories, social media and artificial intelligence will only heighten the systemic nature of cyber risks.

In response to these unique risk factors, cyber insurers began carving out such exposures from traditional property and casualty (P&C) policies and managing them via standalone insurance products, allowing for more appropriate coverage and accurate pricing.

The inclusion of incident response services like forensic investigation, legal advice and public relations, notification and credit monitoring costs improved the insured's experience in the immediate aftermath of a breach while greatly reducing overall claim costs. First-party coverages for data destruction and extortion (i.e. ransomware) and third-party coverages for network security, media liability and Payment Card Industry lawsuits became available. Business interruption clauses were clarified to address losses resulting from non-physical damage, and contingent business interruption wording was broadened to include the interruption of a shared computer system such as a cloud provider or data hosting service. New endorsements for businesses and industries with unique cyber exposures began to appear.

However, these first standalone cyber insurance policies were designed primarily for large, global corporations with dedicated risk management and IT staff, large cybersecurity infrastructures and huge budgets.

Many small and medium businesses, which often lack dedicated insurance or cybersecurity expertise, did not understand which coverages they might need, what cybersecurity standards must be in place to ensure valid claims are paid or what to do in the event of a breach. Applications were long and complex, underwriting was punitive for those without robust cybersecurity and detailed incident response plans and policy wordings were confusing.



CYSURANCE AS A SERVICE: (CAAS)

Perhaps most importantly, the claims process was slow and tedious for any company lacking the technical capabilities to quickly and transparently prove a loss occurrence, verify security protocols and provide detailed evidence to claims adjusters.

Since business interruption makes up 36% of the cost of a cyber breach according to the FBI's Cost of a Data Breach Report, 2019 and lost business has been "one of the largest expenses of a cyber breach" for the past four years, getting claims paid and systems back online can greatly reduce a company's overall loss.

To address this gap in the market, platforms targeting small to medium businesses began to emerge in the 2010's touting online enrollments, affordable premiums, broad coverages and an array of cyber-security services. These platforms began to ease the cyber insurance buying process for growing companies and sought to improve insurability by offering them security services to mitigate risks before a breach, however friction points still existed for customers.

Many of these providers were not licensed insurance agents – meaning they didn't "have the pen" of the insurer underwriting their policy and could not actually bind policies without the carrier's approval. This often resulted in business owners getting a 'soft' quote online only to discover they had to then speak with a third-party broker and answer additional underwriting or security questions to finalize coverage and price. Without a proprietary policy or pricing matrix, protections also varied from policy to policy, endorsements were often needed – for additional premium – to avoid gaps in cover, and costs could fluctuate drastically depending on the insuring clauses needed or the applicant's cyber risk management infra-structure.

CYSURANCE AS A SERVICE: (CAAS)

In addition, these insurtech startups often focused their technology solutions on front-end, pre breach cybersecurity.

While correct in understanding the need of growing businesses for external expertise in this area, they did not account for the rise of Managed Service Providers (MSP) – and subsequently, Value-Added Resellers – in this space. In the early 2000's, these out-sourced information technology and security providers began providing remote monitoring and management software and followed with mobile device management, managed security and remote firewall administration. Such vendors quickly established themselves as the leaders an market experts in this field, with the market expected to grow at a CAGR of 11.1% between 2017 and 2022.

At Cysurance, we've listened to the market and leaned on our background in risk intelligence, cybersecurity, information management and policy expertise to offer an alternative cyber insurance model: Cysurance -as-a-Service (CaaS). A simple, technology-empowered platform that offers all the coverages a growing business needs for one low price, without application or underwriting, and is bundled with MSPs' products and services to reduce friction. .

With complete online delivery, CaaS helps business owners easily implement an innovative cyber insurance program that improves claim outcomes and business resiliency.

To develop this innovative platform, we partnered with Chubb, a leading provider of cyber risk solutions backed by the financial strength of an A++ balance sheet. Together we created a proprietary policy made up of a broad base form including first-party, third-party and cybercrime and hand-picked endorsements of particular use for small and medium businesses, such as coverage for reputational damage, system failures, and human error. In the event of a loss we'll pay for upgrades to cybersecurity to avoid similar future claims, and if an insured's client requires indemnity for cyber risks under a written contract, they are automatically covered.

Using an exclusive pricing matrix, we then eliminated applications and underwriting.

The only information needed to quote a policy is the insured's industry and revenue. Then, with a few simple attestations and confirmation of basic cyber-security infrastructure like antivirus software – which can easily be verified by the customer's MSP if needed – coverage can be bound. This unique feature is available because Cysurance is a licensed insurance agent in 49 states and Canada, with further geographic expansion coming. In all, a business owner can quote and bind a robust cyber insurance policy in less than 3 minutes, completely online. Yet the true value of CaaS is in its ground-breaking use of technology to speed recovery after a breach and a suite of easily-bundled products designed to meet any need or budget. Rather than reinvent the wheel, Cysurance leverages the best-in-class security and monitoring technologies already provided by MSPs to flag anomalous network activity. The associated forensic data and code is then recorded in a blockchain, providing detailed, irrefutable evidence of the event.

This greatly reduces time and expense in verifying a loss and determining the source and extent of the breach during claims adjustment.

Simultaneously, a smart contract created upon enrollment automatically launches an incident response team to begin remediation. In most cases, the insured will be contacted by their breach response coach before even knowing the breach has occurred, again saving time and money in the event of a claim.

Of course, none of this matters, if it's not delivered in way that eases adoption and administration. With CaaS, MSPs become a Cysurance Sponsor to access a wide range of solutions that bundle with their existing software and cloud-based products, seamlessly delivering holistic cyber risk management.

With CaaS, You CAN now Offer Confidence as a Service Solution

Beginning with a Silver sponsorship, vendors can offer our simplest most affordable product, RansomProtect. All that's needed is a client list and a credit card. That's $25,000 of immediate, automatic ransomware protection each for clients of any size, in any industry. Sponsors can cover the cost for their customer OR resell it as a marked-up bundle with existing offerings, giving you a branded, streamlined, value-added solution that increases client "stickiness".

For sponsors looking to offer more robust protection, our Gold and Platinum programs offer additional Ransom-Protect licenses, help create a clear journey for customers to upgrade coverage through our Essential and Complete policies and provide your sales team with bespoke sales and marketing support. Gold and Platinum sponsorships also offer increased revenue opportunity through Royalty Fees for each enrolled customer and Service Fees you can add as a line item in your monthly billing.

To make sure our service provider sponsors have options – not to mention the insurance coverage they need to protect their own unique cyber risks – Cysurance also offers our Tech E&O product.

Purchase of a Tech E&O policy automatically grants Platinum sponsor status and provides full cyber liability insurance PLUS coverage for your professional liability arising from general tech-nology services.

For MSPs looking for a way to differentiate their businesses and increase recurring revenue, or growing businesses looking to manage their cyber risk and safeguard their future, Cysurance-as-a-Service delivers broad, affordable insurance coverage in minutes via a simple, online platform.

CYSURANCE AS A SERVICE: (CAAS)

By leveraging the trusted relationships and security infrastructure of technology providers, we can focus our technology on improving the claims experience and reducing financial damages from a cyber breach.

Finally, cyber insurance has caught up to the high-tech world it seeks to protect.

Kirsten Bay
CEO - Cysurance
kbay@cysurance.com

Cysurance is the next-generation cyber solution, protecting small businesses and their partners through affordable cyber insurance. Built on a proprietary platform, our program comes with a complete set of features to safeguard business continuity and insure against loss, protecting both revenue and recovery.

For more information, visit www.cysurance.com, follow us on LinkedIn, Facebook, Instagram and Twitter, or email us at info@cysurance.com.

cysurance