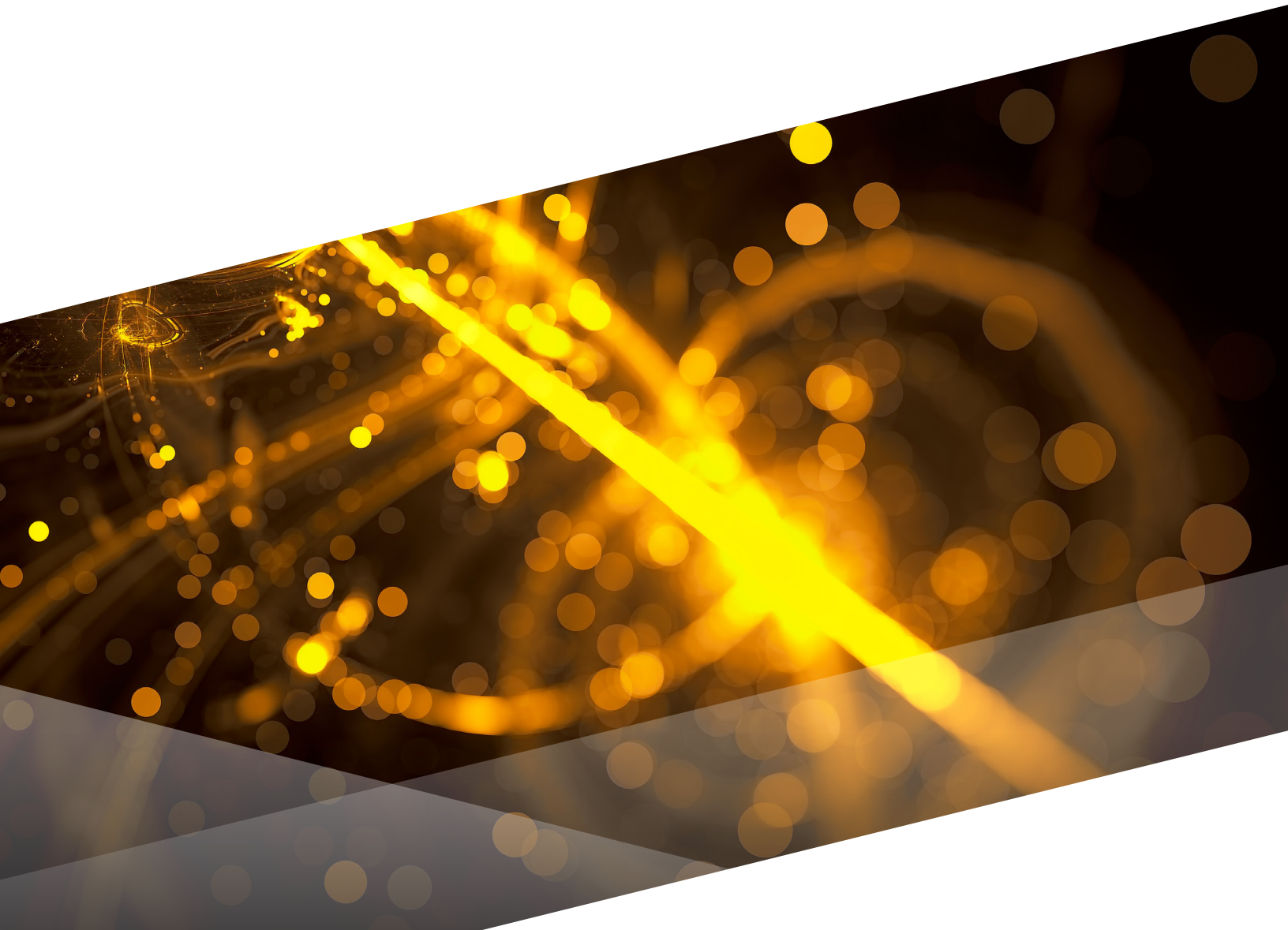
Cyber Catalyst by Marsh

INSIGHTS | MARCH 2020

Cyber Catalyst℠ 2020 Risk Outlook

Top 5 Cyber Risks for 2020



INSIGHTS | MARCH 2020

Cyber Catalyst 2020 Risk Outlook

CONTENTS

Organizations are spending an ever increasing amount on cybersecurity, with the aim of reducing the impact of cyber risk. That's axiomatic in business: allocate dollars to a critical problem, with the expectation it will yield results.

In the US, cybersecurity spending is forecast to top $160 billion in 2020, a 60% increase over 2014, and is estimated to reach $230 billion in 2025. But even as cybersecurity budgets soar, the economic impact of cyber-crime is escalating. The global cost is now estimated at $1 trillion.

The Need for a Different Approach

Organizations are frustrated: they expect their cybersecurity spending to deliver performance improvements similar to those delivered by investment in other areas of enterprise risk. And business leaders increasingly recognize that investing in technology alone is not sufficient, and that cybersecurity budgets cannot continue to grow without limit.

When it comes to choosing how to allocate cybersecurity dollars, organizations are often equally challenged by the crowded and complex cybersecurity market, with thousands of products and services on offer, all claiming to help manage cyber threats. Many organizations lack the expertise or resources to identify which are the most effective and appropriate for their needs.

Cyber Catalyst – A Beacon of Clarity

In 2019, Marsh teamed with leading cyber insurers to create Cyber Catalyst℠, an innovative program designed to help clients and other organizations that are searching for significance in their cybersecurity choices. Cyber Catalyst provides organizations with clarity and actionable intelligence they can use to make more informed decisions about which cybersecurity solutions to adopt. The program brings together eight cyber insurers to evaluate and identify cybersecurity solutions they believe can help reduce cyber risk. In the 2019 program, 17 cybersecurity products and services received the 'Cyber Catalyst' designation.

Looking Back on 2019 and Ahead to 2020

Following the program's strong first year, we are taking a look back at the most important cyber risks that insurers participating in Cyber Catalyst saw in 2019 – not just the loss figures, but their insights and experience from working with thousands of insureds.

The insurers have also identified the top five cyber risks they expect to see in 2020, and the types of solutions addressing those risks that they encourage vendors to submit for evaluation in Cyber Catalyst this year.

This connection is one of the key value drivers for the Cyber Catalyst program: The insurance industry is helping organizations to not only identify and respond to cyber risks, but also to take proactive steps to adopt meaningful solutions and practices that can improve their cybersecurity posture and reduce the damage from cyber events. Cyber Catalyst does not aim to replace other sources of cybersecurity evaluation or to signal that technology alone is enough. Instead, it leverages the unique insights of leading cyber insurers to deliver a new, important perspective on how organizations can incorporate truly impactful cybersecurity products and services into a comprehensive cyber risk management program.

The 2020 Cyber Catalyst program opens for submission of eligible products and services in March.

For more information, contact cybercatalyst@marsh.com or visit www.marsh.com/cybercatalyst.com.

2019 Risk Landscape

Insurers participating in Cyber Catalyst identified the most notable risks affecting their insureds and resulting in claims in 2019. Chief among these were ransomware attacks, which increased in frequency, severity, and breadth of victims. The evolution of ransomware was a particular concern: we've seen a shift from relatively unsophisticated, low cost attacks, to highly sophisticated attacks that target vulnerable organizations, exfiltrate or corrupt data, and demand payment of tens or even hundreds of millions of dollars. Today's ransomware has shifted well into the realm of the criminal economy.

Data breaches remained a significant risk in 2019, particularly costly "mega" breaches affecting millions of records. The **2020 Allianz Risk Barometer** cites the average cost of managing a mega breach at $42 million, up 8% over the previous year.

Business interruption also ranked as a considerable and growing risk, with claims and loss figures often lagging initial breach and ransomware claims due to the challenges of measuring and documenting the incident's operational and economic impact.

Other major cyber risks seen by the Cyber Catalyst insurers in 2019 include: **social engineering**, often in the form of **business email compromise attacks** which use phishing or other means to dupe users. Human error was identified as a consistent vulnerability, with insufficient policies, training, and employee awareness often opening the door to threats that technology alone could not prevent.

Outside of cyber-crime, privacy regulation was named as a small but growing risk in 2019, with a few participating insurers citing claims stemming from the **Biometric Information Privacy Act** (BIPA), and most forecasting the emergence of wrongful data collection as a looming risk for the year ahead.

Finally, a common theme cited by the insurers was that of system and technology **configuration errors**, or misconfiguration of cybersecurity tools that leaves gaps for hackers to exploit. Faulty configuration was often cited in conjunction with cloud risk, but also related to the incorrect or incomplete installation and integration of controls and other technologies.

AXIS

"One sophisticated ransomware attack on a global manufacturing client encrypted and prevented access to multiple production lines and IT systems. We provided access to legal experts to advise on regulatory obligations and technical advisors to bring systems back online and reverse engineer the encryption keys, enabling full recovery. In addition to covering those costs, we advised the client to increase incident response testing and implement bespoke back-up solutions for critical systems."

— AXIS

beazley

"We saw a rise in business email compromise, especially in the US, where a single language and large population create more attack surfaces and an easier environment for phishing or fraudulent emails. We also saw a large amount of non-malicious incidents such as accidental disclosures and misconfiguration."

— BEAZLEY

Munich RE

"Topping the list of 2019 risks were business interruption events affecting clients in the large industrial space. Whether the attacks impact factory lines or are distributed across IT or OT systems, the result is downtime. Losses were not catastrophic as with NotPetya or WannaCry, but we helped many insureds respond to BI attacks. It's a concern that's driving insurance uptake among large industrials."

— MUNICH RE

MARSH

"Ransomware and data breach were the leading cyber risks affecting our clients in 2019. We saw significant increases in both the frequency of ransomware attacks and in the amounts demanded. Equally troubling, ransomware attacks are often causing business interruption events as companies incur income loss and extra expense to mitigate the attacks. Data breaches are still prevalent, as 2019 headlines showed, and financial exposures are rising as new privacy regulations come on line. Our focus in 2019 and going forward is helping clients understand how cyber threats are evolving and build cyber resilience."

— MARSH

"The frequency and severity of ransomware claims spiked tremendously: It was the number one loss event in terms of ransom demands and level of forensics required. However, we see many insureds responding to the threat by changing back-up procedures. So claims that could easily have been $250,000 became $15,000 because of the defensive actions taken and work with our expert incident response vendor partners. We also saw an increased number of claims for business email compromise, social engineering, and violations of BIPA."

— AXA XL

"A few mega-breaches in 2019 will result in claims payouts totaling tens of millions of dollars. The frequency of such breaches has not increased, but they will likely continue to occur. We saw ransomware events more than double in 2019, with extortion demands averaging in excess of $300,000. And where ransomware claims used to involve just extortion and forensics costs, the large majority now also involve business interruption claims, which can take six to seven months to resolve. Business Interruption proof of loss can be a challenging concept."

— SOMPO INTERNATIONAL

"In 2019, we saw many incidents among industry classes that are not traditionally big purchasers of cyber insurance, such as manufacturing and construction. Data breach risk has historically driven cyber insurance buying, but events of the past two years – NotPetya and others – have raised awareness about business interruption risk and the loss protection offered by cyber insurance."

— ZURICH NA

"One of the biggest risks we saw in 2019 was human error: It continues to be a top vulnerability that requires constant training and repetition. Training addresses human imperfection, and companies should take it seriously – it's easy to implement. It's also a sign that the company is risk aware and usually more knowledgeable about their overall cyber risk program."

— ALLIANZ

"In the last year, the CFC cyber claims team handled more than 1,500 incidents and witnessed a sizeable jump in ransomware and extortion events, nearly doubling in frequency between 2018 and 2019. What's more, not only were these events much more frequent, but they were also disproportionately expensive — even though they accounted for 31% of our cyber claims in terms of frequency, they accounted for 39% of what was paid out."

— CFC

International claims rose **13%** in 2019. Top risks affecting our clients: Data breaches and technology/media liability events.

— *AXIS*

Beazley Ransomware Milestones 2018

- Highest ransom demand reported: **$8.5 million**
- Highest ransom paid: **$935,000**
- Average demand/payment: **$116,324**

*Beazley Breach Briefing 2019

"Ransomware and social engineering comprised just over **60%** of claims in 2019, including a large increase in ransomware attacks on manufacturing and chemical companies."

— AXA XL Real-life cyber claims scenarios 2020

2020 Risk Outlook — Top 5 Risks

Cyber Catalyst participating insurers agreed on the top five cyber risks they expect to dominate the threat landscape in 2020. Some are evolutions of those seen in 2019, exacerbated by an increasingly sophisticated and aggressive threat environment. Others derive from heightened scrutiny or pressure on how organizations manage their data practices, vendor relationships, and integration of new technology, and the vulnerabilities that are subsequently exposed. In each case, the risks are not static or wholly predictable but dynamic, and will continue to evolve throughout 2020 and beyond.

Ransomware

Cyber Catalyst insurers said ransomware attacks will continue in 2020, given the relatively low entry hurdle for many hackers and increasingly large sums demanded.

Many of the conditions that have fostered the growth of ransomware are expected to remain constant during 2020.

"It's logical to believe ransomware will continue in 2020, because hackers find it profitable and many companies have proved to be not as secure as they should be. Insurers are likely to demand more security around ransomware, and coverage is standard in most policies now."

— ALLIANZ

"Businesses continue to be increasingly reliant on technology and adopt more and more physical devices, so there are an ever growing number of attack surfaces. In addition, barriers to entry are limited, and ransomware is a crime that is very difficult to police."

— AXIS

"We're seeing the commoditization of tools and knowledge around ransomware, so the cost of entry is nearly zero, and attacks on organizations without strong cyber security defenses will likely continue or increase. Sophisticated hackers are also increasingly targeting high value entities with novel strains of ransomware that add a 'doxing' threat of public exposure or shaming."

— BEAZLEY

The insurers emphasize, however, that ransomware will continue to morph in 2020, with attackers taking more risk and acting more strategically.

"Ransomware is now an industry where criminal syndicates target companies using several attack vectors. Companies that have not invested in endpoint protection or info security to an appropriate degree will be at risk, whether small or large. Large firms that think, 'we're a manufacturer, no one wants our data' are just as vulnerable as PII companies."

— SOMPO INTERNATIONAL

"Threat actors will likely escalate the recent practice of exfiltrating data, then releasing ransomware into the system environment, and threatening to publish data on the internet. They're now taking the data, not just freezing it."

— AXA XL

"It's a step-change in the ransomware ecosystem: Where attacks were once mass distributed at random, now attackers are analyzing the economic potential of where the attack has penetrated and sell that information for criminals to exploit. We will see more targeting of susceptible companies, and more foresight by attackers about the potential value of the target."

— MUNICH RE

"Cybercriminals are getting savvier when it comes to ransomware. We expect the proliferation of Ransomware as a Service (RaaS) to continue to drive frequency and severity."

— CFC

Privacy Regulation/ Data Collection

The California Consumer Privacy Act (CCPA) took effect January 1, 2020, and many subject organizations – for-profit entities that collect data of California residents – are still in the process of understanding how it impacts them and the requirements for data collection and use. The CCPA contains provisions for potentially significant legal damages as well as regulatory fines for non-compliance.

As with the EU General Data Protection Regulation (GDPR) and BIPA, the scope of CCPA extends beyond incidents involving data breach, to business data practices. Legal action or regulatory enforcement could be taken for wrongful data collection that does not involve breach or data disclosure.

"With CCPA coming online, we expect an uptick in privacy events and claims around how companies collect and use data, even when the data is secure. Regulators, consumers, the plaintiffs' bar, all have heightened expectations for companies to be transparent about data collection, so there will be more claims opportunities. It's not just about the perimeter – companies need to have and enforce clear policies."

— MUNICH RE

"It's a call for stronger data practices hygiene by all subject companies. Based on 2019 requests from insureds trying to understand whether they need to comply with BIPA, CCPA, and GDPR and how to come into compliance, we expect help with regulatory compliance will continue to be a big ask by companies in 2020."

— AXA XL

"Now is the time for organizations to review their practices and ask: 'We can and do collect this data, but should we? Is the risk greater than the value?"

— BEAZLEY

The CCPA, BIPA and GDPR are just the start of a growing global privacy regulatory movement, and several US states have similar regulation pending. Given the increasingly stringent regulatory environment and expanded scope around non-breach events, privacy regulation and data collection are likely to be major sources of risk and potentially insurance claims in 2020 and beyond.

"CCPA is the great unknown. We don't expect to see claims until enforcement begins in July, but as with BIPA claims in 2019, wrongful data collection doesn't require breach – it's about enterprise data handling practices."

— ALLIANZ

"Most companies need help understanding how CCPA will impact them and what resources and solutions are available. We're out in front of that, with risk engineering services that help companies prepare to be regulatory ready and a policy that evolves with emerging cyber risk."

— ZURICH NA

"As the world moves to adopt stronger privacy regulation, customers and individuals are increasingly aware of their rights, and businesses are challenged to keep pace with changing requirements around data handling practices. This is a potential recipe for further claims activity in the privacy and data collection area."

— AXIS

"While we expect the CCPA to incite more interest in cyber cover, much in the way that the GDPR did, it is the burgeoning extraterritorial nature of privacy regulation that is going to make it harder for global firms to navigate safely."

— CFC

Supply Chain/ Vendor Management

Organizations have long sought to streamline operations to focus on core competencies and outsource non-core tasks to gain competitive advantage. In an increasingly technology reliant, interconnected business environment, this means granting access to more vendors and devices across the digital supply chain. And the number of vulnerabilities and attack surfaces grows in tandem with growth of networked business partners and devices.

The risk extends beyond breach to business interruption, which can have a material economic impact if production, inventory, or distribution systems are paralyzed or incapacitated. The risk posture of a company's vendors and suppliers is as critical to its security as its own defenses, as hackers are increasingly exploiting the opportunity for multiple points of access to penetrate high value targets.

"Cost savings is one of the key drivers of outsourcing services to the supply chain, but it's important not to do so based on cost alone. Outsourcing to save money without considering the full risk implications is likely to bring additional risks."

— BEAZLEY

"Hackers know it's often easier to attack a target via its vendor network than head-on: Why knock down the front door when the window is easier? Businesses are starting to recognize this and to consolidate the number of vendors, but vendors who view themselves as low risk often have cybersecurity postures that don't measure up."

— AXA XL

"Digital supply chains help companies get products out more efficiently and quickly, but security needs to keep pace. As businesses move from static servers to cloud to digital third-party connections, it's critical to bridge any security gaps."

— MUNICH RE

"Supply chain is a major exposure but it's hard to evidence controls. We are seeing business interruption events at service providers resulting in losses to insureds. If your vendor who you rely upon to conduct your business is down, you're at risk for loss."

— SOMPO INTERNATIONAL

Cloud Migration

More companies are moving to the cloud to decrease their use of costly on premise infrastructure or to maximize efficiencies, which can bring an increase in – or increased recognition of – operational risk. Often it is the migration itself, and the effort to integrate cloud services with systems and data, that is the source of risk rather than the cloud itself. Most of the breach events seen by Cyber Catalyst participating insurers can be ascribed to failure to correctly or completely secure to the cloud environment, not the cloud itself. Common problems can include legacy servers, patching errors, lack of encryption, unsecure S3 buckets, and difficulty managing an abundance of technologies and digital assets. Cloud migration that is executed without careful planning and expertise often creates new, unforeseen risk exposures.

"Cloud integration is key: Infrastructure and implementation is an issue 'at the seams' where discrete technology comes together at points of operation, and it's often the weakest point. Recognizing that vulnerability and taking actions to address it is important."

— MUNICH RE

"The moral of the cloud story is configuration. If you're configured poorly in your own network, it probably means you won't be correctly configured for cloud. It's important to not just check the box; how you implement and use the cloud is almost more important in terms of risk management."

— SOMPO INTERNATIONAL

"With the move to Office 365 and other cloud solutions, many organizations fail to realize that the protections put in place 20 years ago don't necessarily work effectively in today's working environments, which permit both remote access and the use of personal devices. Many times we see organizations that have migrated to the cloud don't use multi-factor authentication (MFA), or turn off MFA for executives – the very people who are targets."

— BEAZLEY

Social Engineering

Social engineering attacks, already a notable risk in 2019, are predicted to continue increasing in frequency, sophistication, and loss size in 2020. One of the most common forms of social engineering seen by Cyber Catalyst insurers is business email compromise: the use of compromised email credentials or a spoofed email address to trick employees into sharing sensitive data or diverting invoice payments.

Social engineering emails on the whole are increasingly cunning, with attackers sending emails from seemingly legitimate senders that feature equally believable design and content to obtain credentials. They are also increasingly focused on fraudulent money transfers, intercepting and altering emails regarding forthcoming payments so that funds are transferred to attackers instead of the rightful payee.

Business email compromise worldwide losses since 2016: **$26 billion**.

— 2020 Allianz Risk Barometer

"Fraudulent invoice instructions are increasingly on the rise. Often those emails are obviously fake, but people tend to trust email beyond rational sense. Even quite sophisticated organizations and employees often assume that IT is checking and screening email traffic, and they trust email requests that they would not in any other format."

— BEAZLEY

"Insurance markets have readily responded over the past few years to expand and add risks such as social engineering under affirmative cyber coverages rather than under other policies where the perils didn't really belong. Social engineering used to be considered a crime coverage, as was invoice manipulation."

— AXA XL

"Average cost of a business email compromise claim in 2018: **$70,960**."

— Beazley Breach Briefing 2019

— AXIS

Cyber Catalyst 2020 – Solutions Sought

Insurers participating in Cyber Catalyst identified a range of cybersecurity solutions they believe will be important to help organizations address the five critical risks they expect during 2020. While the Cyber Catalyst 2020 program will accept for evaluation all eligible cybersecurity products and services, participating insurers are particularly keen to see solutions – ranging from "hard" technology tools to "soft" services – that can help organizations prevent, mitigate or manage risks in these areas:

- "**Training programs:** a good training program should be holistic in approach and focus on securing the data, how you secure devices and computers, and where you store your data – not just the clicked link. That's only the vector."
- "Wrongful data collection applies to the policies of the enterprise, not its cybersecurity controls. We'd like to see tools or services to help **manage wrongful data collection**, and to advise on changing privacy regulations along with best practices for regulatory compliance."
- "Services that can help insureds **increase their regulatory awareness** and assess their exposures in this area. Many private companies don't see themselves as targets. A service that could also help insureds adapt their data collection and handling policies to ensure full compliance would be particularly useful."
- "Products that can help companies **identify perimeter weaknesses** would be great: remote desk protocol (RDP) or Telnet exposed to the internet are often overlooked and lead to breaches, or organizations expose insecure protocols to the internet without realizing it. A security scorecard would be advantageous for 2020."
- "Services that address **human risk**. IT tools, firewalls, server controls all are valuable, but staff education and training are arguably of more value. We need solutions to help overcome the psychological barrier that sees training as a mandatory checklist. Compulsory training modules need to adapt to the modern environment: Doable on the phone, at home, as a game, tied to rewards, personalized, and relevant to real life situations. If you can get employees motivated and fully engaged, then you've got thousands of extra eyes and ears mitigating your organization's cyber risk profile."
- "**Data protection services** will be highly important for 2020, as regulators are ready and active in levying fines for existing regulation and new ones like CCPA that are coming online. We're looking for solutions that are effective, regardless of the ultimate outcome on insurability of fines."
- "Capabilities that help with **data management interpretation** – providing insight to help understand what's going on internally with an organization's data, and visibility into broader global and regional trends. Continual risk assessment monitoring would also be highly useful; not just a single point in time, but over time."
- "More **tools for SMEs** would be great – not every company can afford big ticket security tools. Detection response tools or managed security service provider services would fill a real need."
- "There is big demand for systems and services that **automate information security**, both because companies want to reduce headcount in that area, but also reflecting the dearth of skilled cybersecurity professionals. Demand far outpaces supply for those roles, and organizations who cannot attract the talent are likely willing to pay for the automated capability."
- "Solutions that are **easy to configure and deploy**. Products that get these aspects right take a lot of the hard work away from the user, which usually leads to better implementation and a more satisfied and secure organization."

Role of the Cyber Catalyst Program

Cyber Catalyst participating insurers believe the program plays an important role in bridging the gap that frequently exists between the realms of cyber insurance and cybersecurity, and in helping organizations more confidently identify tools and products that are effective in strengthening their cybersecurity posture.

The insurers also emphasized how the goals of Cyber Catalyst dovetail with their own efforts to help insureds strengthen cybersecurity programs and how meaningful solutions can inform the risk underwriting process.

"Cyber Catalyst helps bring the insurance and cybersecurity worlds together to create a common viewpoint that helps the end user. Building cohesion between insurers and cybersecurity providers can be really valuable in terms of improving risk outcomes. Cyber Catalyst delivers tangible value – it's not an innovation award or a rubber stamp, but a rigorous, meaningful process that results in actionable information."

— MUNICH RE

"In the midst of today's cybersecurity 'gold rush', where there is a huge market with lots of players and options, it can be hard to identify the tools and providers that really work or have proven expertise. Cyber Catalyst requires candidates to demonstrate that their products solve actual problems. Like insurers' vendor panels, Cyber Catalyst helps CISOs and others sort through the crowded cybersecurity arena."

— AXA XL

"As insurers, we have skin in the game, and we're accountable to our insureds. Cyber Catalyst puts us in the position of helping drive accountability of cybersecurity providers and products on behalf of our insureds. Cybersecurity should be a team sport: Cyber Catalyst helps identify products that truly perform and vendors interested in working as a team to address risk."

— MUNICH RE

"Cyber Catalyst helps bring transparency to the underwriting process, which is sometimes a hurdle for potential buyers. It highlights factors that we underwriters look at in terms of how you protect your company and your ecosystem, and shows that we believe the use of effective technologies can help you better manage cyber events. By identifying those technologies, Cyber Catalyst delivers real value for companies that lack the resources to do that on their own."

— ZURICH NA

"Cyber Catalyst reflects an evolution of how insurers look at risk. Where traditionally insurance paid for losses post-occurrence, we now also aim to proactively help our insureds strengthen risk postures and prevent loss at every instance, across the risk continuum."

— ALLIANZ

"Organizations want the best possible protection against fast-evolving cyber threats, but many struggle to navigate the crowded cybersecurity marketplace. With Cyber Catalyst, our clients and other organizations can have greater confidence that they are implementing cybersecurity tools that can have a meaningful impact on reducing the cyber risks they face."

— MARSH

Cyber Catalyst 2020 — Leveraging Insights of Insurers

The Cyber Catalyst program adds the collective voice of leading cyber insurers to the dialogue surrounding approaches to cyber risk management, with the aim of helping improve overall cyber risk management outcomes.

Cyber insurers have considerable experience and insight in the area of cybersecurity and solutions that have a meaningful impact on reducing cyber risk. The insurance industry has responded to the costliest, most catastrophic cyber events of the past decade, paying hundreds of millions in cyber event losses annually.

"Insurers are focused on helping insureds improve their cyber risk profile, not just reacting to risk. Services like training and tabletop exercises, and advisory on security systems, access controls – that is all part of our broad risk management offering to clients."

— ALLIANZ

"Outside of law enforcement and the largest breach response providers, insurers arguably have the most first-hand knowledge of what breaches occur and what they cost. We also play a pivotal role in our insureds' cyber practices: We incentivize the adoption of beneficial behaviors and actions to strengthen cybersecurity. We invest in credentialed cybersecurity professionals with technical expertise to evaluate cybersecurity programs, products and providers, and share that information with our insureds."

— AXA XL

"Insurers have the advantage of seeing many cybersecurity programs and gaining a really good feel for what's effective or not, and which technologies are being effectively utilized. Larger insurers can bridge the perception gap – to see the events that may not make the news but still impact businesses. That macro perspective of cybersecurity on a portfolio level is hard to find outside the insurance industry or large-scale tech services firms."

— AXIS

Beyond paying losses, however, cyber insurers bring a wealth of knowledge and broad perspective on best practices that the Cyber Catalyst program seeks to tap into for the benefit of organizations seeking insight. These insurers also offer a host of value-added services and resources that can help clients and other organizations not only respond and recover from cyber events, but better prepare for and mitigate the risk.

"The interests of insurers are fully aligned with those of insureds: Reducing the cost and impact of risk. If we can provide a service that will reduce your risk, if we can help you avoid spending money on a tool that isn't really effective, then we've delivered real value. We can see where cybersecurity money is well spent and generating measurable ROI for our insureds. We are an ally of our insureds."

— BEAZLEY

"Insurers are uniquely positioned: We have both an intimate view of our insureds' exposures and security posture, and a 30,000-foot view of the global market that enables us to identify trends in emerging risks, best practices, cybersecurity providers and products, and response mechanisms. Often the bespoke programs and unique solutions we create for large insureds become standard options benefiting the broader marketplace."

— MUNICH RE

"We can help companies quantify potential losses from cyber events and tie them directly to insurance limits. We know where the cyber losses are coming from, and we're able to recommend certain controls that can help our insureds. And through our vendor panel, we give insureds access to the best vendors we know, and help them manage their costs."

— SOMPO INTERNATIONAL

"We have a macro perspective across our entire portfolio, so we see how companies are affected by cyber events like business interruption and reputation harm, not just losses. We can offer best practice recommendation on risk prevention as well as response. With our risk assessment reporting, we give risk managers the right vocabulary to engage with other key stakeholders about ways to improve response time, deploy resources more effectively, and strengthen program maturity."

— ZURICH NA

Cyber Catalyst Designated Solutions 2019

Seventeen cybersecurity solutions received the Cyber Catalyst℠ designation in the inaugural Cyber Catalyst by Marsh℠ program. Participating insurers identified these products and services as being able to have a meaningful impact in reducing cyber risk.

Cyber Catalyst℠ 2019 Designated Cybersecurity Solutions

Aruba Policy Enforcement Firewall	BigID Data Privacy Protection and Automated Compliance
CrowdStrike Adversary Emulation Penetration Testing	Crowdstrike Falcon Complete™
Digital Guardian Data Protection Platform	FireEye Email Security
FireEye Endpoint Security	Forescout Device Visibility and Control Platform
HackerOne Bounty	HPE Silicon Root of Trust
KnowBe4 Security Awareness Training and Simulated Phishing Platform	Mimecast Security Email Gateway with Targeted Threat Protection
Perspecta Labs SecureSmart™ critical infrastructure monitoring solution	RSA SecurID® Access
Trustwave® DbProtect™	Virsec® Security Platform
Zingbox IoT Guardian™	

Evaluation Criteria

Insurers participating in Marsh's Cyber Catalyst program evaluated cybersecurity solutions that address major risks, including data breach, business interruption, data theft or corruption, and cyber extortion. In evaluating these solutions, insurers used six criteria:

1. *Reduction of cyber risk:* demonstrated ability to address major enterprise cyber risk such as data breach, theft, or corruption; business interruption; or cyber extortion.
2. *Key performance metrics:* demonstrated ability to quantitatively measure and report on factors that reduce the frequency or severity of cyber events.
3. *Viability:* client-use cases and successful implementation.
4. *Efficiency:* demonstrated ability of users to successfully implement and govern the use of the product to reduce cyber risk.
5. *Flexibility:* broad applicability to a range of companies and industries.
6. *Differentiation:* Distinguishing features and characteristics.

Evaluation and Designation Process

The platform for vendors to submit cybersecurity solutions for evaluation was open from March 26 through May 5, 2019. Eligibility criteria required that the cybersecurity products or services be 1) currently available in the United States and 2) deployed in an enterprise environment. The evaluation process included a deep dive into eligible products and services that participating insurers felt merited review, and demonstrations to those insurers.

The eight participating insurers voted independently on each solution, with Marsh tallying the votes and Microsoft serving as technical advisor. Cyber Catalyst designation was awarded to products receiving positive votes by at least six insurers. Neither Marsh nor Microsoft participated in the Cyber Catalyst[SM] designation decisions.

The next Cyber Catalyst program cycle is expected to launch in 2020, when cybersecurity solutions can be submitted for evaluation.

Insurance Policies and Implementation Principles

Organizations that adopt Cyber Catalyst-designated solutions may be considered for enhanced terms and conditions on individually negotiated cyber insurance policies with participating insurers. Marsh has worked with each participating insurer to establish endorsement wordings that reflect the coverage enhancements that those insurers might offer to Marsh clients which adopt one or more Cyber Catalyst designated solution.

When considering potential policy enhancements, those insurers will expect organizations to implement the Cyber Catalyst designated products or services in a certain manner. To that end, participating insurers worked with the vendors whose solutions are Cyber Catalyst designated to develop "implementation principles" for each product or service.

Contact Marsh at cyber.risk@marsh.com to learn more.

CLARITY IN A CROWDED CYBERSECURITY MARKET

Cyber Catalyst by Marsh[SM] brings together leading cyber insurers, with technical advice from Microsoft, to evaluate and identify cybersecurity solutions they consider effective in reducing cyber risk. Cyber Catalyst is designed to help organizations make more informed choices about cybersecurity products and services to manage their risk. It provides organizations with greater clarity and confidence in an increasingly complex cybersecurity marketplace, as well as an understanding of which cybersecurity solutions most matter to insurers.

Cyber Catalyst: Sparking Change in Cyber Risk Management

Cyber Catalyst by Marsh[SM] is a first-of-its-kind program designed to help organizations make more informed choices about cybersecurity products and services to manage their cyber risk. Through Cyber Catalyst[SM], Marsh brings together leading insurers to identify cybersecurity solutions they consider effective at reducing cyber risk — giving organizations greater clarity and confidence in an increasingly complex cybersecurity marketplace.

The Cyber Catalyst by Marsh[SM] program provides organizations with a clearer understanding of which cybersecurity solutions matter to cyber insurers. Participating insurers include Allianz; AXA XL, a division of AXA; AXIS; Beazley; CFC; Munich Re; Sompo International; and Zurich North America, which collectively represent a substantial portion of gross written premiums in the $5 billion global cyber insurance market. The insurers' evaluation focuses on better equipping organizations to select cybersecurity solutions that can have a meaningful impact on cyber risk.

Challenges of Navigating the Cybersecurity Market

Organizations want the best possible protection against fast-evolving cyber threats, but often struggle to optimize the impact of their cybersecurity investments. Even as corporate cybersecurity budgets grow, the economic impact of cyber events continues to climb. The annual cost of cybercrime is estimated at $1 trillion globally, and is rising every year. Although companies want to see meaningful risk reduction results from their cyber dollar, many are challenged to identify the most effective solutions.

That's because the cybersecurity market can be crowded, complex, and difficult to navigate. Global spending on cybersecurity is expected to top $150 billion in 2020. Thousands of cybersecurity firms offer products, services, and solutions designed to mitigate and combat cyber risk, but it can be challenging for individual organizations to evaluate those offerings given limited corporate resources and expertise.

Cyber Insurers Have Valuable Insights to Offer

Cyber insurers have responded to the most catastrophic and costly cyber events of the past decade. They also have considerable experience and insight gained from their engagement with a wide range of cybersecurity vendors and products. This experience means cyber insurers are well-positioned to provide informed views on the potential effectiveness of cybersecurity solutions in reducing cyber risk.

How Cyber Catalyst℠ Works

The Cyber Catalyst℠ program was created by Marsh to help address questions we often hear from clients: "What cybersecurity solutions should we implement?" "What cybersecurity products does our insurer value most from a risk underwriting perspective?"

In Cyber Catalyst℠:

- Cybersecurity vendors submit their eligible products and services for consideration and evaluation.
- Participating insurers evaluate cybersecurity offerings and identify those they believe can have a meaningful impact on major cyber risks, such as data breaches, business interruption, data theft or corruption, and cyber extortion.
- Marsh facilitates but does not contribute to the decision-making process or evaluation of cybersecurity solutions.
- Products and services considered by participating insurers to be effective at reducing cyber risk are designated as "Cyber Catalyst℠".
- Organizations that adopt Cyber Catalyst℠–designated products and services may qualify for enhanced terms and conditions on individually negotiated cyber insurance policies offered by participating insurers.

Vendor Application Information

Any cybersecurity vendor who meets eligibility criteria is invited to submit their product or service for evaluation in the Cyber Catalyst℠ program, provided the product or service is offered in the United States.

The application period for cybersecurity vendors to submit products and services for evaluation in the 2020 Cyber Catalyst program is March 10th through 27th.

Marsh Cyber Risk Practice

For more information on the **Cyber Catalyst℠** program or vendor eligibility and evaluation criteria, visit marsh.com/cybercatalyst, email us at CyberCatalyst@marsh.com,or contact:

THOMAS REAGAN
Cyber Practice Leader
Marsh
+1 212 345 9452
thomas.reagan@marsh.com

marsh.com/cybercatalyst

SM Cyber Catalyst SM

Cyber Catalyst by Marsh℠

Leading insurers participating in the 2020 Cyber Catalyst program collectively represent a substantial portion of the $5 billion global insurance market. They are:

Allianz · AXA · AXIS · beazley · cfc · Munich RE · SOMPO INTERNATIONAL · ZURICH

MARSH

Marsh is a global leader in insurance broking and innovative risk management solutions, and a leading broker of cyber insurance. Marsh's global cyber risk management practice places more than $1 billion in premiums annually for more than 6,300 clients worldwide.

Cyber Catalyst by Marsh℠

The 2020 Cyber Catalyst program will be open for submission of eligible products and services March 10-27, 2020. Cyber Catalyst product designations are expected to be announced in September.

For more information, contact cybercatalyst@marsh.com or visit www.marsh.com/cybercatalyst.com.