REUTERS EVENTS™

NASTY BYTES: MANAGING DIGITAL RISK IN ENERGY TRANSITION BUSINESSES

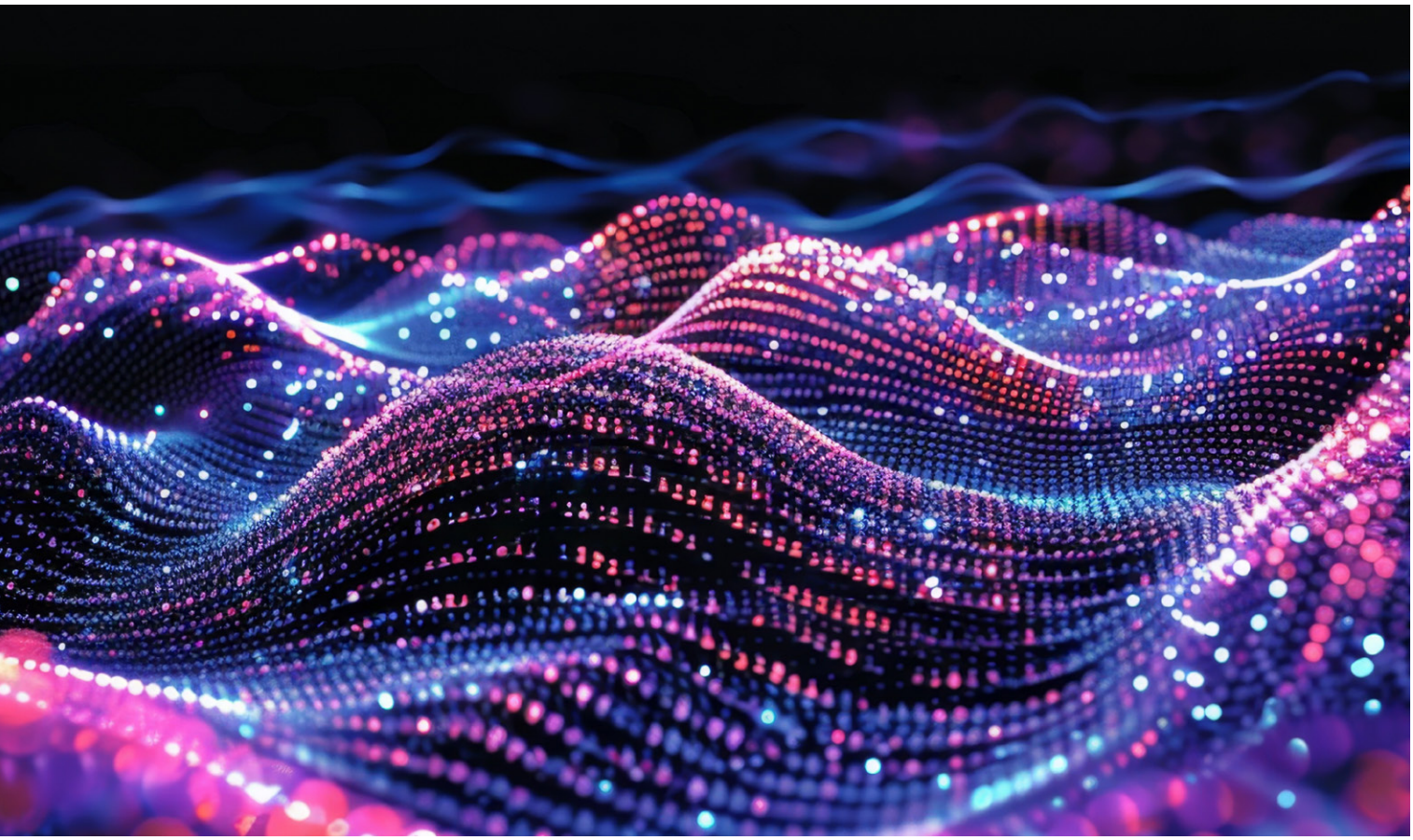
October 2024

In association with

AXA

XL Insurance Reinsurance

CONTENTS



RENEWABLES-LINKED CYBERSECURITY FEARS GROW AS ENERGY TRANSITION ENCOURAGES FIRMS TO GO DIGITAL

August 2024 saw the United States Department of Energy (DOE) releasing a solar power-focused tech security tool amid fears of cyberattacks on renewable energy infrastructure.

The launch of the DOE's SolarSnitch system, which is designed to safeguard communications in photovoltaic equipment,[1] followed a U.S. Federal Bureau of Investigation (FBI) private industry notification in July that warned of increasing cyber risks for clean energy companies.

"Structural shifts in the reduced cost of implementation of renewable energy and incentives for development of clean energy have created new targets and opportunities for cyber threat actors to disrupt and exploit for their own gain," said the FBI.[2]

Cybersecurity is also a growing concern for Europe's energy transition businesses, with companies including EnBW of Germany and Hydro of Norway looking to bolster defenses as the conflict between Russia and Ukraine heightens the threat level in the region.[3]

Because of their distributed nature and often relatively small scale, solar parks, wind farms and battery storage systems have traditionally been viewed as less of a cyber security risk than legacy energy infrastructure assets such as oil refineries and nuclear power plants.

But that perception is changing, says Michelle Chia, Chief Underwriting Officer for Cyber, Design and Select Professional Markets at insurer AXA XL, AXA Group's specialty, property and casualty arm.[4]

Unlike legacy assets, which are often managed using manual processes and specialized operational technology, the energy transition is heavily reliant on IT systems that are vulnerable to cyberattacks, she says.

"Because the energy transition relies so heavily on digital technology, it's even more critical to have cyber resilience," Chia says.

AS WELL AS HACKERS, DIGITALLY ENABLED ENERGY COMPANIES FACE A GROWING THREAT LANDSCAPE

An August 2024 attack on U.S. oilfield services firm Halliburton's north Houston campus[5] illustrated how hackers prize energy infrastructure's potential to deliver juicy rewards.

Yet while large oil companies will always be a target for cyber threats, smaller, more digitally enabled firms also face risks because they may be easier to penetrate from outside.

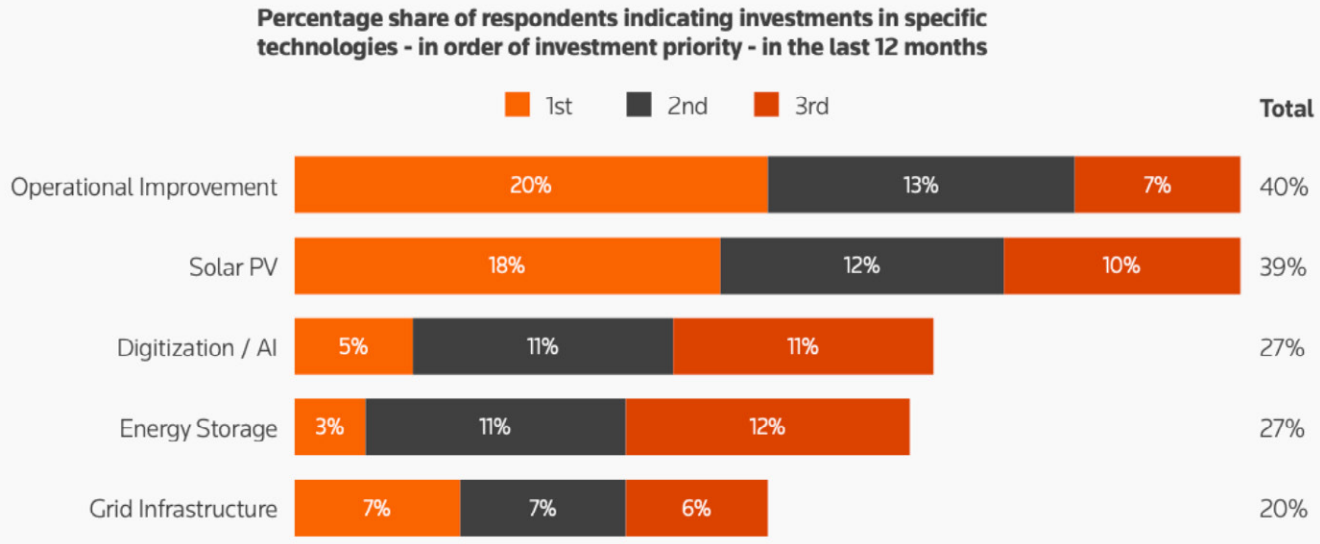
And as IT security provider CrowdStrike demonstrated in July 2024, it does not even take a hacker to bring down a connected business. A glitch in a CrowdStrike software update ended up crashing more than 8 million computers[6] in what has been described as the biggest cyber outage in history.[7]

The software being updated was designed to foil hacker attacks and prevent IT system downtime. "It's not just an attack that causes a system outage," says Timothy Smit, Global Head of Cyber Risk Strategies and Partnership Programs at AXA XL.

"There are risks that renewable energy companies have not considered outside of 'if we have a ransomware attack, what does it do to us?'"

DIGITIZATION IS THE THIRD HIGHEST AREA FOR ENERGY TRANSITION SPEND IN 2024

Reuters Events reader database respondents' five most cited technology investment areas in 2024.



Source: Reuters Events Energy Transition Survey, 2024.

A general lack of IT resilience, coupled with insufficient operational and business resiliency, significantly increases the risks facing clean energy companies that lack sophisticated cybersecurity measures, Smit notes.

All too often, access to devices in solar farms and wind parks is via common or default usernames and passwords, and communication is via unprotected radio bands that can easily be intercepted—on purpose or otherwise.

Cyber-related business interruption claims arise from a mix of malicious activity and non-malicious human error, he says, including instances where plant operators themselves have caused an outage.

"The operational technology is old and while they're replacing it, sometimes the system shuts down," Smit says. "[Operators] don't realize the new system won't integrate with the old systems, creating an issue."

As distributed, low-carbon generation increasingly dominates electricity production in western markets, renewable energy company bosses need to prioritize IT resilience, Smit believes.

"Our clients know a cyber event is serious, but we think there is often more that can be done to avoid them, which is good for their business continuity and reduces overall risk—exactly the business we're in," he says.

CYBERSECURITY RISKS DEMAND THAT ENERGY TRANSITION BUSINESSES MERGE WITH CARE

The extent to which energy infrastructure is vulnerable to cyberattacks was underscored in February 2024 when a government security advisory warned a Chinese state-sponsored group had already infiltrated U.S. systems.

The U.S. Cybersecurity and Infrastructure Security Agency said Volt Typhoon hackers had compromised the IT environments of multiple critical infrastructure organizations, including energy companies, in preparation for a major crisis or conflict with the United States.[8]

That energy infrastructure is at risk from sophisticated nation states is nothing new, says AXA XL cybersecurity expert and Global Chief Underwriting Officer Libby Benet, who lists the threat as one of the top three cyber 'danger zones' facing renewables companies.

"Energy infrastructure is often a target in conflict," she says. "Also, nation states are hacking into energy infrastructure to steal intellectual property, for example finding the spec on a turbine, or to make copies of advanced tech."

As well as this, there is another cyber danger zone that clean energy company leaders may be less aware of, paying large sums of money for it.

"In a renewable energy market characterized by different sizes and scales of businesses, many of them involved in mergers and acquisitions, a new acquisition can lead to issues," Benet explains.

A situation she says AXA XL has seen several times is where a big company buys a smaller rival, doesn't do due diligence on cyber risk, "and the small company's lesser security leads to a breach in the larger organization."

A third danger area is a lack of cybersecurity in supervisory control and data acquisition systems. "These run on firmware and they're often the last thing to get updated regarding security," says Benet.

"It's fine if operating offline, but the hunt for meaningful insights from big data means assets are increasingly operating online in connected networks, leaving assets vulnerable."

Reflecting growing insurance industry concern over industrial control system vulnerabilities, AXA XL invested in specialist cyber risk management company DeNexus in 2023 and 2024.

DeNexus offers an end-to-end cyber risk management platform that energy companies can use to prioritize cybersecurity investments and reduce risk. The product leverages cybersecurity tools already deployed and "empowers users to assess their top cyber risk drivers, measure the potential losses that may arise from a cyber event in financial terms and prioritize risk mitigation projects," says DeNexus.[9]

INSURERS STEP UP CYBERSECURITY ROLE AS PART OF THE GLOBAL TRANSITION TO CLEAN ENERGY

Growing evidence of cyber vulnerabilities in the clean energy sector is leading insurers to step into a role traditionally reserved for technology providers. AXA XL, for example, not only offers cyber insurance but also provides tools, services and resources to identify, mitigate and respond to threats.[10]

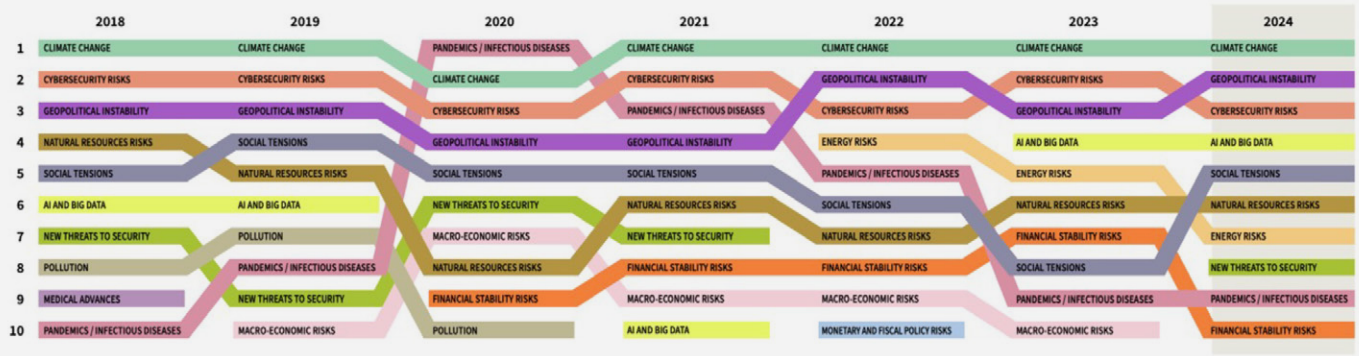
"We are experts in helping organizations increase their resilience, cyber or otherwise," says AXA XL's Michelle Chia.

"AXA is making significant investments in building out our cyber insurance capabilities, whether that's on the risk transfer underwriting side or the advice and risk engineering side, because we recognize that cyber is a critical component for organizations' ability to conduct business as usual."

The insurance industry's desire to safeguard the energy transition is underscored by the results of the 2024 AXA Group 'Future Risks Report' that has seen experts ranking climate change as the biggest risk in the world for six out of the last seven years.[11]

CYBERSECURITY VIES WITH CLIMATE CHANGE AS A TOP GLOBAL RISK

Evolution of expert perceptions of top global risks, from 2018 to 2024.



Source: AXA Future Risks Report, 2024.[12]

Cybersecurity has consistently ranked second or third and "continues to be seen as a major threat," says AXA Group in the report.[13]

"Concern about this risk is likely closely linked to geopolitical instability, alongside continued progress in the capabilities of artificial intelligence and increasing dependency on large providers," it says.

For companies involved in the energy transition, "we're creating a cyber risk consulting team that proactively talks with our clients about best practices, helping guide those clients to follow and adopt a centralized framework," says Timothy Smit of AXA XL.

Practicing and following a pre-approved script can make a big difference to outcomes in the event of a cyber incident, says Chia. When CrowdStrike's software update crashed computers worldwide, some companies were able to restore operations within hours. Meanwhile, Delta Air Lines struggled for days to restore service, cancelling more than 6,000 flights and losing an estimated $500 million.[14]

"When it relates to cyber, organizations can have a plan of the types of things that can happen—and when something does happen, actually follow the plan," Chia says.

INSURANCE SEES CLEAN ENERGY COMPANIES "AT A FORK IN THE ROAD" ON CYBER RISK AWARENESS

Getting clean energy leaders to engage more deeply with cybersecurity is key as renewables become the mainstay of global power systems, AXA XL believes.

"We are at a fork in the road where there is awareness that cybersecurity is critical for the resilience of organizations because of our reliance on digital information or operational technology," says Chia.

"There is an opportunity, since energy transition companies are newer, to keep cybersecurity top of mind when they build infrastructure."

Without this mindset, there is a real danger that clean energy-based grids could be brought down by bad actors, or even innocent faults.

The insurance industry is well placed to help mitigate cyber threats because it underwrites much of the risk involved and can see where the main threats lie, says Chia.

With U.S. renewable energy companies only having experienced cyber threats in the last half decade,[15] "it's a new sort of risk relative to fire, which we've had since the caveman," Chia says.

Given limited experience of cyber risks, "it's really important to get the trend on a scaled basis," she says. "Insurance companies have the benefit of that."

Insurers hope that by helping their clients have a better grasp of cyber risks, they will be able to improve the chances of surviving an attack or similar incident. "Something like 60% of small business organizations go out of business within six months of a cyber event," warns Chia.[16]

Reducing that figure, and other losses associated with it, could help curtail insurance payouts—and premiums.

CONCLUSION

When one pictures an IT threat, the at-risk entities that come to mind are government agencies, retail outlets or financial institutions — not solar parks in green fields or wind farms far out to sea. That image may need to be revised.

While renewable energy infrastructure has not yet suffered unduly from cyber threats, the growing ubiquity of its projects, digital nature of its equipment and lack of controls in its supply chains and mergers all point to an increasing risk of planned or unintentional incidents.

The insurance industry is aware of this problem and is taking steps to deal with it. But insurers cannot act alone. Energy transition companies, too, must give cyber resilience the priority it deserves, and they must do so quickly, since the failure that brings down the grid could be just seconds away.

REFERENCES

1. Anna Ribeiro, Industrial Cyber News, August 21, 2024: DOE debuts SolarSnitch technology to boost cybersecurity in solar energy systems. Available at https://industrialcyber.co/threats-attacks/doe-debuts-solarsnitch-technology-to-boost-cybersecurity-in-solar-energy-systems/.

2. Anna Ribeiro, Industrial Cyber News, July 2, 2024: FBI warns of increased cyber threats to expanding US renewable energy sector. Available at https://industrialcyber.co/threats-attacks/fbi-warns-of-increased-cyber-threats-to-expanding-us-renewable-energy-sector/.

3. Nora Buli, Nina Chestney and Christoph Steitz, Reuters, June 15, 2023: Insight: Cyberattacks on renewables: Europe power sector's dread in chaos of war. Available at https://www.reuters.com/business/energy/cyberattacks-renewables-europe-power-sectors-dread-chaos-war-2023-06-15/.

4. AXA XL is a division of the AXA Group that provides products and services through three business units: AXA XL Insurance, AXA XL Reinsurance and AXA XL Risk Consulting.

5. Liz Hampton, Reuters, August 21, 2024: Top US oilfield firm Halliburton hit by cyberattack, source says. Available at https://www.reuters.com/technology/cybersecurity/top-us-oilfield-firm-halliburton-hit-by-cyberattack-2024-08-21/.

6. Jonathan Stempel, Reuters, August 1, 2024: CrowdStrike is sued by shareholders over huge software outage. Available at https://www.reuters.com/legal/crowdstrike-is-sued-by-shareholders-over-huge-software-outage-2024-07-31/.

7. Packetlabs blog, July 22, 2024: CrowdStrike: What the Biggest Cyber Outage in History Teaches Us About Incident Response Plans. Available at https://www.packetlabs.net/posts/crowdstrike-what-the-biggest-cyber-outage-in-history-teaches-us-about/.

8. Cybersecurity and Infrastructure Security Agency cybersecurity advisory, February 7, 2024: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure. Available at https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

9. DeNexus press release, December 4, 2023: DeNexus Expands Access to its AI-Powered Cyber Risk Assessment Platform. Available at https://blog.denexus.io/resources/denexus-expands-access-to-its-ai-powered-cyber-risk-assessment-platform.

10. AXA XL website, 2024: Cyber. Available at https://axaxl.com/insurance/product-families/cyber.

11. AXA XL, October 14, 2024: Future Risks Report, 11th Edition. Available at https://www.axa.com/en/news/2024-future-risks-report.

12. Ibid.

13. Ibid.

14. Rajesh Kumar Singh, Reuters, August 7, 2024: Microsoft blames Delta for its struggle to recover from global cyber outage. Available at https://www.reuters.com/technology/microsoft-blames-delta-its-struggle-recover-global-cyber-outage-2024-08-06/.

15. Sean Lyngaas, CyberScoop, October 31, 2019: Utah renewables company was hit by rare cyberattack in March. Available at https://cyberscoop.com/spower-power-grid-cyberattack-foia/.

16. Joe Galvin, Inc, May 7, 2018: 60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack. Here's How to Protect Yourself. Available at https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html.

DISCLAIMER

The information contained herein is intended for informational purposes only. Insurance coverage in any particular case will depend upon the type of policy in effect, the terms, conditions and exclusions in any such policy, and the facts of each unique situation. No representation is made that any specific insurance coverage would apply in the circumstances outlined herein. Please refer to the individual policy forms for specific coverage details.

The report presented here is researched and written by Reuters Events™ and is intended to engage readers on topics of emerging risk. Therefore, the report reflects the viewpoints of the authors and are not necessarily the views of nor are described risks necessarily underwritten by AXA SA or its affiliates.

Clicking on the link button of other providers opens external websites. Since AXA SA and its affiliates have no influence on the design and content of the linked pages, including sub-pages, it cannot assume any guarantee or liability for the information presented on these pages. In particular, AXA SA and its affiliates are not obliged to periodically check the content of third-party offers for illegality or criminal liability.

We specifically disclaim any warranty or representation that compliance with any advice or recommendation in any document or other communication will make a facility or operation safe or healthful, or put it in compliance with any standard, code, law, rule or regulation. Save where expressly agreed in writing, AXA SA and its affiliates disclaim all liability for loss or damage suffered by any party arising out of or in connection with our services, including indirect or consequential loss or damage, howsoever arising. Any party who chooses to rely in any way on the contents of this document does so at their own risk.

The information has been established on the basis of data, projections, forecasts, anticipations and hypotheses which are subjective. This analysis and conclusions are the expression of an opinion, based on available data at a specific date. Due to the subjective aspect of these analyses, the effective evolution of the economic variables and values of the financial markets could be significantly different from the projections, forecast, anticipations and hypotheses which are communicated in this material. There can be no guarantee that any strategy presented will be implemented or ultimately be successful.

These scenarios are presented as of this document's date. They do not constitute a representation or guarantee as to future scenarios nor performances. AXA SA and its affiliates disclaim any and all liability relating to these scenarios' description and can modify these scenarios according to market evolutions and taking into account the regulations in force.

May be subject to change without notice. AXA SA and its affiliates expressly disclaims any responsibility for (i) the accuracy or completeness of third party data (ii) the accuracy or completeness of the models, assumptions, forecasts or estimates used in deriving the analyses, (iii) any errors or omissions in computing or disseminating the analyses or (iv) any uses to which the analyses are put.

This summary does not constitute an offer, solicitation or advertisement in any jurisdiction, nor is it intended as a description of any products or services of AXA SA or its affiliates. All insurance products, including the applicability of coverages, limits and exclusions, are subject to their full terms and conditions. AXA XL is a division of AXA Group providing products and services through three business groups: AXA XL Insurance, AXA XL Reinsurance, and AXA XL Risk Consulting. In the US, the AXA XL insurance companies are: Catlin Insurance Company, Inc., Greenwich Insurance Company, Indian Harbor Insurance Company, XL Insurance America, Inc., XL Specialty Insurance Company and T.H.E. Insurance Company. In Canada, insurance coverages are underwritten by XL Specialty Insurance Company - Canadian Branch. In Bermuda, the insurance company is XL Bermuda Ltd. Coverages may also be underwritten by Lloyd's Syndicate #2003. Coverages underwritten by Lloyd's Syndicate #2003 are placed on behalf of the member of Syndicate #2003 by Catlin Canada Inc. Lloyd's ratings are independent of AXA Group. Not all of the insurers do business in all jurisdictions nor is coverage available in all jurisdictions. Information accurate as of October 2024. AXA, the AXA and XL logos are trademarks of AXA SA or its affiliates. © 2024