Infrastructure's insecurity issue

High profile attacks have pushed physical safety and cybersecurity to the fore, Anne-Louise Stranne Petersen, Isabel O'Brien and Daniel Kemp write. As the number and source of these risks keep changing, so do the costs of keeping critical infrastructure secure

As billions of bubbles of natural gas made their way from the wreckage of the Nord Stream pipeline to the surface of the Baltic Sea, we were all suddenly and brutally reminded that keeping infrastructure safe is of paramount importance.

However, the fact that infrastructure is vulnerable should have come as no surprise to anyone directly invested in it. Infrastructure has always been a target for those who wish to inflict pain on a society, and with more people having easier access to means of destruction, threats of damage, physical as well as internet-based, loom ever larger for the asset class.

With a book and film called *How to Blow Up a Pipeline* making waves in popular culture, and nation-states sponsoring what amounts to cyber-war, what is an asset manager to do to stay on top of these threats?

Infrastructure Investor has probed this dilemma by talking to developers, lawyers, insurers and GPs, and has found that, though risks are on the rise globally, they are still manageable. For now.

How to be prepared

Europe wasn't prepared for war and limited consideration had been given to keeping infrastructure assets secure. Russian ships had been mapping out the Baltic and North Seas and critical power generation facilities in full view of

Infrastructure Investor
Infra under attack
Cyber-crime is no longer the only threat
PEI

Cover story

anyone who bothered to look both before and after the invasion of Ukraine.

Some of Europe's onshore wind facilities took an immediate hit. As Russia launched its invasion, a cyberattack, which in all likelihood had not targetted renewables assets, disrupted the satellite communications that remotely monitored and controlled 5,800 Enercon wind turbines, making them inoperable for months as Enercon worked to replace communications hardware.

It is difficult to imagine what owners of these assets could have done to prepare, and this notion of ultimately being defenceless against attacks is palpable in discussions with GPs.

Carsten Koenig, managing director of European infrastructure at Partners Group, which is invested in Dutch offshore wind, says: "The next discussion regarding the protection of infrastructure, specifically critical infrastructure, is where the responsibility of an operator or an investor ends and where the responsibility of the public or the government begins."

The issue is pertinent because offshore wind farms are designed to prevent accidents, rather than defend against attacks; the cables are buried deep in the seabed to protect against anchors or fishing, rather than bombs.

"How much resilience do we ask of investors in infrastructure and operators of infrastructure?" asks Koenig. "You can always ask for more expensive hardware and software measures. That will come at a cost. And then the question is, how do we ensure the business case is still there for infrastructure operators and investors?"

Who should pay?

Part of what investors need to understand is the current and future role of public institutions, and Koenig envisions that the discussion could turn outright political.

"At the moment, [regulatory demands for security] is not killing the business case. But if governments were to ask for a higher level of resilience, we would certainly need to find a mechanism to compensate existing investors and operators for that. Because if you have taken the financial investment decision, your business gets locked in. Most infrastructure investments will not have compensation in their revenue line or EBITDA line automatically to meet additional demands for capex. We will then need to discuss how to incentivise or at least compensate for additional levels of protection."

Initiatives such as joint EU maritime patrols to see off potential Russian saboteurs of marine infrastructure have been launched following evidence that the Russians have scouted Dutch and Belgian offshore wind installations. There is also a potential North Sea nations pact in the making on jointly protecting infrastructure.

But this does not impress everybody. The CEO of Ørsted's Germany division, Jörg Kubitza, says Germany is not doing enough to address the issue. "At the moment, it is still completely unclear where our duties end and where the duties of the security authorities begin," Kubitza says, adding that Poland protects its offshore substations with military assets and onshore control centres with armed personnel.

According to the recent World Economic Forum *Global Risks Perception Survey*, the risk of terrorism and interstate conflict could not effectively be managed by businesses. And the notion that public-private co-operation would be useful was nixed too.

Koenig agrees with this: "If a higher level is needed at some point, and you need marine troops around the wind farms, that is on the public side of what needs to be done."

Counting on the government

The debate on how to square private ownership of critical infrastructure assets with the public need to keep them secure is global. In Australia, persistent tension with China has led to changes in legislation and sharpened the focus on security, while the US has arguably been in a state of war since 9/11 and the subsequent passage of the Patriot Act. Even so, protecting infrastructure from criminality, damage or – whisper it – confiscation is not straightforward.

"For the threats that we know about to date… I think the federal government is doing a reasonably good job," says Maria Lehman, US infrastructure lead at engineering consultancy GHD, as well as the vice-chair of the National Infrastructure Advisory Council. "I think once you get down to other layers

"I think the insurance industry is looking at security hard, harder than the finance industry is looking at it"

MARIA LEHMAN
GHD

of government, it's very patchy on what we're doing. It's all about trying to figure out what the next threat is... This is a constantly changing dynamic that you've got to deal with. For some sectors, the security may not be as high as it should be."

Using a strategy straight from the Cold War handbook, limits to foreign ownership of or involvement in key assets have been imposed. Chinese companies, in particular, are increasingly prohibited from investing in infrastructure in OECD countries. In the UK, this has meant buying out state-owned China General Nuclear from the coming Sizewell C nuclear power plant. However, CGN remains invested in the 3.2GW Hinkley Point C plant under construction.

The US has limited Chinese investments in subsea cables, and several governments have decided to exclude or limit the penetration of Huawei's technology in the wider communications infrastructure space.

In a similar vein, Australia has introduced strong controls with foreign investments, recently blocking a Chinese investment in a rare earths producer. Generally, the Australian government is strong on oversight.

This is not a problem, says Edward Lloyd, deputy CEO of Foresight Australia: "The new legislation and amendments for the Critical Infrastructure Act place positive obligations on asset owners. I don't see them as unreasonable, only as a regulatory layer that everyone needs to be aware of and comply with."

However, all oversight comes at a cost to a business's autonomy, as well as its purse, says Belinda Harvey, partner at law firm White & Case. "There are significant and increasing obligations around compliance and, in particular, the reporting functions associated with this, which impinges on the ability of infrastructure owners to operate unconstrained in a way that is to the benefit of the asset and potentially their shareholders."

Insurers are wising up

There is general agreement among those consulted that the cost of insurance is going up, and terms are changing too as insurers grapple with the changes to the risk environment. Insurers usually do not insure losses resulting from war, terrorism and sabotage, but they are in uncharted territory and there is some leeway on physical damage caused by cyberattacks.

"In the last couple of years," explains Andries Veldstra, senior underwriter at GCube Insurance Services, "we have seen more cyberattacks, and the insurance market has responded – as insurance markets do – by trying to reduce their exposure by introducing exclusionary language. However, after the exclusion, it is possible to reintroduce some cover, called buyback, for physical losses resulting from cyberattacks."

This may not last. "If the Ukraine war continues and the threat increases in our own North Sea region, we will see more hard exclusionary language," he says, and the reason lies in the re-insurance market.

"As direct insurers, we are heavily dependent on specific re-insurance markets, for instance with NAT CAT [natural catastrophes] insurance and the political violence market. When they withhold cover or capacity, we can't offer products, and this has meant the addition of more exclusionary language over the past few years."

Though not all risk is insurable, adequate insurance is about more than money, says Michael Kolodner, global renewable energy leader at insurance broker and risk adviser Marsh Specialty.

"If we think about insurance as simply risk transfer, we limit the role that insurance plays. It is not just about the policy limit or the amount of the risk that has been transferred; it is also about

what we learn as we go through the process of transferring and managing that underlying risk," says Kolodner.

As the cost of insurance goes up, there are more benefits to being proactive on security. Insurance works best at certain points of the probability-and-severity-of-loss curve and is not necessarily the solution to every risk that an organisation faces.

"Some of our clients spend considerable sums on hardening the security of their infrastructure because the return on that investment is ultimately better than paying insurers for insuring something that is within their ability to control," Kolodner explains.

He is anything but sanguine about the risks to the energy system, calling the grid "the most complex machine ever created on the planet".

"One of the things that keeps me up at night is that we are integrating new technology and new assets into our energy ecosystem at a pace never seen before. This is fraught with risk."

Security and the business case

With all of this additional risk, can infrastructure keep its reputation as being a low-risk asset class?

According to Fran Faircloth, partner and core member in US law firm Ropes & Gray's cybersecurity practice, the answer is no. "I think it's changed the way investors look at critical infrastructure or at infrastructure as an asset class generally, because it's traditionally been considered a low-risk asset class and now it has become a target of these attacks. That increases the risk profile and it's something that has to be considered."

Overall, though security takes up more of GPs' time and money, it is not clear that the issue has material impact on business cases. Not surprisingly, the GPs who agreed to be interviewed for this story all have solid governance in place. Foresight is a case in point: "I can't think of any examples where we have not invested [in an asset because of security concerns]. But now, when we're going through due diligence and screening assets, our focus is on making sure we understand the risk profile and how security fits in with that," says Lloyd.

"The costs haven't had a material impact on our portfolio returns," says Daniel Timms, head of asset management Australia and New Zealand at Igneo Infrastructure Partners. Igneo makes use of a specialist cyber, intelligence and investigations firm, in addition to the portfolio companies' cyber-risk management systems. "Obviously, that has a cost, but that cost is a fraction of what the potential impact could be if we didn't manage this risk appropriately."

The focus on risk ensures that any company board that dreams of making it into an infrastructure fund's portfolio had better pay attention to security, according to Philippe Camu, chairman and co-chief investment officer of infrastructure at Goldman Sachs Asset Management: "For infrastructure businesses, protecting physical assets and ensuring continuity of operations in the face of various threats is usually a core part of the business. The management team's proven expertise in navigating these challenges can be an important part of our investment decision."

William Greene, managing partner at Stafford Capital Partners, says there is even a silver lining to the shift in threat levels: "If anything, [the Ukraine war and energy crisis] confirmed our belief in a need for a swift transition away from fossil fuels. It also reinforced our belief in investing in the more stable markets while maintaining wide diversification.

"As we see it, the risk of physical damage to assets through deliberate destructive behaviour is not a systemic risk to the industry, and although such acts generate headlines, we should keep our industry focused on true systemic risks such as climatic change."

Underestimating the risk

Still, despite the confidence on display, the industry could well be in the calm before the storm.

Looking at cybermap.kaspersky.com, one of several companies mapping cyberattacks in real time, Bas Kruimer, business director of digital grid operations at risk management adviser DNV Netherlands, says: "This looks like warfare, doesn't it? And this is ongoing all the time, malicious parties in many countries are constantly trying to break in digitally everywhere around the world."

Omid Rahmani, associate director with Fitch Ratings, uses similar language: "The conflict that's going on in Eastern Europe right now could very

well be the world's first cyber war. And I think that that's going to just become more normalised as time goes forward because those types of attacks are very low risk and very high reward."

Indeed, of risks with the greatest potential impact on a global scale, cyberattacks on critical infrastructure is fifth, after energy supply, cost-of-living, inflation and food supply. This is according to the World Economic Forum's *Global Risk Report*.

For businesses, widespread cybercrime and cyber-insecurity was deemed the fourth most severe risk for the coming two years, after the cost-of-living crisis, natural disasters and geoeconomic confrontation.

Marsh's Kolodner worries that not every part of the financial system has understood the severity of the threat that is cyber-crime.

> *"We have to recognise that no matter how good you think you are today, 12 months from now, you need to be better"*
>
> **TIBOR SCHWARTZ**
> **QIC**

"When we look at standard terms and conditions required from financial institutions, project finance included, cyber-risk does not feature prominently. Notably, organisations can get a loan without demonstrating that they have assessed the asset's cyber-risk. I don't know if that is a conscious or an unconscious choice, but we talk to clients about it. Some clients don't need the bank to ask about risk because they know the risk already. Others don't want the banks to ask because they won't be owning the assets long term, so the problem will be passed on to the utility that will buy the asset. It is not always an easy conversation to have."

Kolodner is not alone in being concerned. GHD's Lehman says: "I think the insurance industry is looking at security hard, harder than the finance industry is looking at it."

Cyber 'a physical threat'

In the infrastructure investor community, focus on cyber has undoubtedly increased over the past few years, and there is an understanding that physical security and cybersecurity are closely linked.

"Cybersecurity can be considered a physical threat," says Foresight's Lloyd. "It is a real risk, and I think it's coming to the forefront of attention for many people at the moment, and certainly something we're very focused on."

However, there is plenty of room for improvement, says Nathan Jones, director of cyber at advisory company AON. "What we've traditionally seen across infrastructure is that cyber-risk is not necessarily understood. Very rarely has a full business impact assessment been completed to fully understand critical business functions – including those that are outsourced to the supply chain – where cyber-risk has been exposed, understood, managed and mitigated. Quite often it is just transferred into an insurance policy. And as the amount of infrastructure assets that

are being exploited by cyberattacks has gone up, the cost of insurance has gone up significantly, particularly over the past 18 months."

He has, though, sensed a decided shift in tone over the past couple of years. "Two and a half years ago, we weren't pushing against a closed door, but discussions with investors were based on them not having been victims of cyberattacks and simply insuring their way through the risk. Now, we are pulled through open doors and having a lot of conversations with investors who have assets and little idea of the cyber-risk, and who are now either not able to or struggle to transfer the risk to the insurance market."

Faircloth agrees: "There's still work that needs to be done to help investors evaluate the risk, because it is something that's still kind of nebulous, but I do think investors appreciate the need to evaluate the risk. What I've seen clients struggle with is how to get all the information they need in a form that's digestible to them as investors to fully understand the risk profile and be prepared and educated."

Advice is also sought by greenfield investors, she says: "There has been a huge step change in terms of GPs, investors, and deal teams asking questions of the contractors during design and build. 'How is this going to work? How do you connect? What governance are you applying? What standards are you accrediting to? What legislation do I need to comply with?' That's still quite a new conversation, but it is happening."

Jones singles out social infrastructure and data centres as two areas that are increasingly under threat from criminals looking to collect a ransom. For social housing, the threat is about the personal data they hold. For data centres, there is a physical risk too.

"I've been involved in projects recently to explore how a data centre was built, who has access to the plans, how the centre is controlled – because if you've got access to the plans, you've got access to how that data centre lives and breathes," Jones says, adding ominously: "A successful cyberattack is quite often one that goes unnoticed until the hacker wants you to know."

> *"Obviously, [investing in security] has a cost, but that cost is a fraction of what the potential impact could be if we didn't manage this risk appropriately"*
>
> **DANIEL TIMMS**
> **Igneo Infrastructure Partners**

The skill-set gap

The price of complacency is high, says Keith Skirbe, managing director within Houlihan Lokey's technology group: "The average cost of a data breach is continuing to increase."

Encouragingly, Skirbe sees signs that the message is getting through despite the tightening economic environment. "I'd say we've definitely seen some pullback in security budget in this macro environment. But the core cybersecurity products and services, there's still strong appetite for spend there."

Feeding that appetite, however, may not be easy. The skills gap in cybersecurity is well documented. A UK government report from 2022 states that 51 percent of UK businesses have a basic skills gap and can't with confidence set up firewalls or detect malware. There is no good reason to assume that this situation is unique to the UK, and the problem comes down to a general dearth of qualified people.

"The skill gap in cybersecurity is growing rapidly, making it difficult to replace cybersecurity personnel and leaving organisations vulnerable," says Fitch Ratings' Rahmani.

This is echoed by DNV's Kruimer: "There is much work to do and not so many people who know how to do it."

Worse still, this gap in skill set comes at what may be an inflection point in cybersecurity as artificial intelligence is now on the cards, says Rahmani: "The rise of third-generation ransomware and the development of AI-powered malware pose new challenges to cybersecurity in critical infrastructure."

At QIC, AI is top of mind too. Tibor Schwartz, senior adviser within the asset management team, says: "What started trickling into the conversations the last year was how artificial intelligence is interacting with the issue of cybersecurity. Clearly, when new and potentially very highly impactful technology comes onto the scene, it can be used for something positive, and also for something quite destructive. We have to recognise that no matter how good you think you are today, 12 months from now, you need to be better."

And that is the crux of the matter on keeping infrastructure secure: this is a perpetual race to stay ahead of the bad actors. How much can any one business do – and be expected to do? At what point does this issue extend beyond board level and enter the realm of national considerations? If and when it does, what will be the costs to businesses of losing a further degree of freedom?

The discussion on how to keep infrastructure secure in a rapidly changing technological environment and geopolitical climate is only just beginning. ■