Inframation News
An Acuris company

IN-DEPTH: CYBERWARS THREATEN TO DERAIL CRITICAL INFRA

25 November 2019 | 12:54UTC

Cybersecurity breaches are set to escalate as operational infrastructure assets move onto digital networks. From high-profile attacks on power grids to telecoms, lack of disclosure may impact M&A valuations while ushering in a new sub-sector for the asset class, reports Katherine Steiner-Dicks

Europe

Country: EU
USA

Published: 25 November 2019

Author: Katherine Steiner-Dicks

With great power comes great responsibility. The famous 'Peter Parker Principle' devised by Spider Man comic book impresario Stan Lee should resonate with any fund manager responsible for assets deemed 'critical' to modern daily living.

The inherent responsibility carried by infrastructure owners and asset managers is spreading across power grids and utilities, altnets and telecommunications, data centres, transport and more recently smart city infrastructure. And much like Peter Parker, adversaries from various nations and backgrounds are all too prepared to commit cybercrimes against heavy industrial owners and the infra funds behind them.

"Critical national infrastructure presents a prize to malicious hackers, which seek to cause interruption and damage to harm the global economy," says Russell Kennedy, Managing Director of Property at Brit Insurance, which partnered with now Carlyle-backed cyber security company Coalfire in 2014 to develop an insurance service to protect companies operating critical infrastructure and industrial machinery from terrorist and other malicious attacks.

The industry-wide digitisation of operational infrastructure assets is a double-edged sword that is also making critical infra "soft targets for adversaries," according to research conducted this year by cyber firm CyberX Labs.

The data shows that industrial control systems continue to have security gaps in key areas such as plain-text passwords (69%), direct connections to the internet (40%), weak anti-virus protections (57%), and WAPs (16%). More than half of all critical infrastructure owners and related industrial companies surveyed in another study (by Forrester Consulting in London last year) have experienced a breach in their industrial control (ICS) or supervisory control and data-acquisition (SCADA) systems.

"Cybersecurity is considered one of the greatest material risks for infrastructure funds and their critical infrastructure investments and assets", says Steven Chabinsky, a partner and the Chair White & Case's Global Data, Privacy & Cybersecurity Practice.

"The issue here is not so much the focus on protecting consumer data, but the potential for entire systems and services to be rendered useless for long periods of time."

Prior to joining White & Case, Chabinsky gathered know-how and solutions, notably as the general counsel and chief risk officer at US cybersecurity firm CrowdStrike but also as a member of the US Commission on Enhancing

National Cybersecurity under President Barack Obama, and as Deputy of the FBI's Cyber Division.

"We anticipate that cybersecurity risk will continue to escalate over the next five years, based on historical precedents," he says. "Companies are becoming increasingly dependent upon technology."

So what's being done about the threat?

"The public nature and media coverage of a number of recent breaches is certainly shining a brighter spotlight on the potential threat," says Charlie Garrood, Aon M&A Infrastructure Leader. "Questioning from LPs and fund managers experiencing cyber-attacks on their own platforms is also heightening the focus [on the cyber threat]," he says, adding that "assessing the exposure across their existing portfolio is also becoming an increasing priority for fund managers as many hold assets which were acquired when the threat level was significantly below current levels."

According to people spoken to for this article, infrastructure funds and investors are now calling on external advisers and cybersecurity experts as part of their due diligence process before acquiring assets but also during asset management.

AI attacks

The Centre for Strategic and International Studies (CSIS), a Washington DC-based research organization, has a 'Significant Cyber Incidents Timeline' dating back to 2006 up to the present day. If the month-by-month run down of some of the global cyberattacks were placed on a whiteboard it might look like a James Bond scriptwriters' brainstorm session.

With a relentless onslaught from hackers with a variety of different motivations, infrastructure owners are now being encouraged to get up to speed on one of the latest trends in hacking: artificial intelligence.

In March of this year, a news service in the US reported how a CEO of a UK-based energy company was fooled by an AI-based software call that impersonated the voice of his German parent company's chief executive. The AI-based voice, urgent in nature with slight German accent and intonation, demanded a transfer of EUR 220,000 be sent to a Hungarian supplier. The company's insurance firm reimbursed the energy company for the fraudulent transfer, but the insurer Euler Hermes Group reported that this was a first-of-a-kind case.

Infrastructure assets can be exposed to a range of cyberattack risks but cases involving power grids and telecom infrastructure have become increasingly prominent over the past few years.

When Britain's energy sector was hacked on 8 June, 2017 – the day of the General Election – reportedly by Russia-backed computer criminals, UK intelligence agency GCHQ had to write a blanket letter to inform the energy sector it likely had fallen victim to the attack. At the time of the attack, several infrastructure funds and limited partners would have been impacted including owners of SGN (Borealis Infrastructure, OTTP, and Abu Dhabi Investment Authority); National Grid owners (Cadent, Macquarie, China Investment Corporation and Qatar Investment Authority, along with fund managers including Hermes and Allianz). Energy networks in Ireland and the Ukraine have also been targeted over the past five years.

Two years later, on the other side of the pond, the first known penetrated grid attack involving a denial-of-service cyberattack was carried out on AES and AIMCo-backed SPower (the largest private owner of operating solar assets in the US).

A vulnerability in the web interface of a vendor's firewall was exploited, allowing unauthenticated reboots of the devices and disconnection between its main command centre and power generation installations. The outages had no impact on generation, but the incident was a wake-up call to owners of critical energy assets and renewables.

"Investors should be well-placed to insist [of their portfolio companies] on a balance between security tools and people. Investment in the human factor can help stop vulnerabilities seen as essential to the security programme,"

an executive in the industry tells *Inframation*.

Much like the geographic spread of infrastructure funds, the breadth of a cyberattack can cross similar borders.

In March this year, a Norsk Hydro industrial-linked ransomware cyberattack (coined 'LockerGoga') started in a US facility and over the course of months, while undetected, affected the entire global organization. Norsk Hydro said that the attack accrued operational and financial losses and costs of up to USD 71m (NOK 650m) and reported USD 3.6m (NOK 33m) in insurance compensation in the third quarter. "Further compensation will be recognized when deemed virtually certain," said the company.

While normal operations did resume, the lessons learned from this event are exemplary.

For one, Norsk Hydro did not pay out a ransom, but instead focused all available internal resources and external expertise to resolve the situation, working around the clock.

The company's transparency of the event has been commended by the Norwegian authorities. The company has even put out a Youtube video about their experience and how they used Facebook and Whatsapp to communicate to 30,000 employees across 40 countries to prevent them logging onto the company's network. The share price even went up, largely due to the company's transparency of the event and working with the media, according to Inger Sethov, Norsk Hydro's head of communications.

Other incidents where critical infrastructure is involved are only being peeled back over time once documents become public.

Regulatory burden

In addition to the direct impact of a cybersecurity event, there also is an increased risk of regulatory enforcement and civil litigation in the aftermath of an incident, not to mention reputational and valuation risks.

"Understanding the potential vulnerabilities in such an emerging and rapidly changing peril, such as cyber risk, is extremely challenging for clients," says Russell. "We have worked with clients to help shape robust cyber security policies, procedures and structures to understand and manage cyber risks. Cyber security expertise, in-house or from third parties, is essential in this, as well as being able to clearly articulate adherence to legal and regulatory frameworks."

For example, the names of US bulk power system entities that violate federal critical infrastructure protection reliability standards – along with identification of standards violated and penalties assessed – may soon be routinely disclosed under changes proposed by NERC and the Federal Energy Regulatory Commission (FERC).

The proposed changes were outlined in a joint white paper published in August. The changes would be made to the format of Notices of Penalty, which NERC issues to violators of Critical Infrastructure Protection reliability standards, by segregating what information can be made public. However, more detailed information that could potentially pose security risks would not be made public.

Increasingly, critical infrastructure regulatory bodies are being pressured by Freedom of Information requests to name those companies that have fallen victim to cyberattacks, and the fines imposed by the relevant regulatory body for any security breaches or loss of service.

UK regulators such as Ofgem and Ofcom have enforcement powers that determine and issue penalties for loss of service, cyber and data breaches. They have sections on their websites with a running tally of those fined. Government authority organisations, such as the UK's Centre for the Protection of National Infrastructure (CPNI), only provide protective security advice.

The insurance industry has helped regulators understand what minimum and appropriate levels of risk are required, say sources.

Cyber valuations

Cybersecurity audits are now essential to an M&A process and can determine the fate of a deal, according to the findings of a survey by the International Information System Security Certification Consortium in the US, a non-profit organisation often known as the world's largest IT security organization.

When performing due diligence, buyers treat cybersecurity programs as an asset, and the vast majority of the 250 US-based professionals with M&A expertise surveyed (96%) consider cybersecurity readiness to be a factor in determining the overall monetary value of the selling company. The survey shows that buyers are "forgiving" to companies that demonstrate they took the right steps to address past breaches, but less so when it comes to previously undisclosed security breaches.

"How can you be an infrastructure fund and not have a full array of cybersecurity protections in place for the critical assets you own?" says Michael Steed, founder and managing partner of Paladin Capital Group, which targets cyber security companies catered to protect critical infrastructure. "You have the accountability as investors in critical infrastructure assets, to have done the investigations of which cyber protection is in place. And if you are a company being bought you have the equal responsibility to show not only that exiting security is in place, but the additional investment that the new investors will have to invest to get the next stage of protection in place," he says.

In today's deal environment, there is real value in undertaking cyber security and data privacy due diligence before a final offer is submitted, says Aon's Garrood.

He warns that unidentified issues can go straight to value, take up significant time to resolve post-close and leave exposures to potentially adverse regulatory implications.

"The lack of cyber incidents disclosed by management in a transaction context is more likely to raise a red flag," says Garrood's colleague Ian McCaw, Aon's Head of Cyber M&A, EMEA. "Cyber M&A experts are able to detect many active vulnerabilities and historic incidents whether or not these have been disclosed by management."

"When a company tells us they have no problems," says Chabinsky, "but concedes that they don't have sufficient technologies in place to discover any problems and that they haven't hired an outside party to look for problems, that concerns us and that concerns our clients."

Inadequate cybersecurity problems could be a sign of other internal weaknesses, yet to be discovered, he adds.

Some of Chabinsky's clients conduct technical diligence using cybersecurity audit firms that typically go onsite. Alongside advisors, the company can determine if they have the qualified personnel or compliance gaps that must be filled to meet industry and regulatory demands.

"As long as management acknowledges shortfalls, we have found more often that buyers seek resolution of material gaps prior to closing than a concession in price. That's different in the context of known breaches, when contingent liabilities such as regulatory investigations and lawsuits may need to be accounted for in the sales price."

Examples of valuations being impacted by cybersecurity breaches are hard to find and infrastructure funds including Ardian, TPG Capital, Macquarie, InfraVia, KKR, and EQT could not be reached or did not make themselves available to be interviewed on the topic.

Outside the sector, it was reported in 2016 that Verizon cut Yahoo's valuation by USD 350m after its 2013 data breach of customer information was revealed and a pay-out fund was on the cards.

Lesley Ritter, Vice President, Moody's Investor Services' Utilities Group, tells *Inframation* that the credit agency has no knowledge of any deliberate "cover-ups" among infrastructure investors or owners, however it adds that in a cybersecurity survey it conducted earlier this year, they did find cyber disclosure varies greatly across sectors and regions.

Within infrastructure, telecommunications companies disclose the most information about their cybersecurity measures, while hospitals and other healthcare providers are "less transparent about their cyber risk oversight and management strategies," says Ritter. For power and energy, Ritter says there is a "regional distinction" between US and European utilities regarding disclosure.

Moody's believes a widespread adoption of standardized reporting and disclosure allows for a more consistent and material assessment of the credit impact-related risks.

"While large European electric integrated utilities provide extensive details about their cyber risk management strategy," she says, "US utilities provide more boilerplate disclosures acknowledging the risk, their board oversight structure, and their access to cyber insurance, but do not elaborate on their enterprise-wide risk management approach."

Investing in cybersecurity

In-house cyber know-how could provide an edge when it comes to valuation and exit for infrastructure funds.

Several infrastructure fund investors have sister fund investments in cyber security companies. They currently include Blackstone which owns Cofense/PhishMe; KKR with KnowBe4 and Optiv Security; TPG (McAfee); Carlyle (Coalfire) and EQT (Open Systems).

Indeed, cybersecurity firms offering outsourced managed services and cloud-based cybersecurity functions ranging from DDoS to endpoint protection are increasingly a potential acquisition target for critical infrastructure companies and funds, says Chabinsky.

Recent examples may include France's nuclear power construction and component company Framatone's take-over of critical infrastructure cyber security firm Foxguard for an undisclosed amount and EQT's ownership of critical back-up power company Coromatic Group, which it sold this year to France's E.ON.

After reaching scale in the infrastructure arena, France's InfraVia Capital Partners is looking to raise EUR 300m for a new fund targeting companies that offer technology solutions for infrastructure assets.

Assets on the line

Investors that have clearly understood the ramifications of revenue loss and regulator-induced fines have ensured that cybersecurity programs and technology are written in contracts ranging from construction, components to O&M services.

Cyber specialists, lawyers, M&A advisors and insurers interviewed for this article all say it would be wise for infrastructure funds to negotiate cybersecurity in all contracts, deals and cyber-event insurance coverage.

A good proxy for infrastructure funds to demonstrate a strong program to others, such as regulators and limited partners, is through third party certifications.

But the fact that a company is certified against a well-known cybersecurity standard does not in and of itself mean that company is secure, warns Chabinsky, though it is a good starting point. Larger companies tend to have dedicated chief information security officers in place with sound qualifications, which also is easy to publicly disclose to partners and regulators, he says.

Cybersecurity is becoming an asset management focus within critical infrastructure portfolio companies and the rising demand following new cyberattack methods will directly correlate with cyber security budgets addressing IT and operational assets and talent.

Governments, infrastructure fund managers and their portfolio companies are expected to work increasingly in tandem by mutually notching up transparency with data sharing.

In the meantime, there are other, less official ways to reinforce cybersecurity. Infrastructure-linked hackathons are just one way that transparency and solutions can be tested, shared and created. Utilities including E.ON have been hosting events regularly to test energy and smart city cyber-protection and get a headstart on best practice. Later this month, Finland will host the first ever 5G Cyber Security Hackathon at Tellus Innovation Arena at the University of Oulu. There may be some infrastructure fund managers in the audience.