Cyber risks within Supply Chains

by **Mauro Signorelli**
Aspen Insurance

Cyber exposure is a serious risk not only to the traditional buyer of cyber insurance – large scale data owners and processers worried about their privacy and data protection liability – but to any business relying on a physical supply chain. Mauro Signorelli, Senior Cyber and Technology Underwriter at Aspen Insurance, looks at why brokers have to work with clients and underwriters to avoid unforeseen gaps in coverage and assess how different policies interact.

The way in which organisations protect information assets, corporate networks and manufacturing systems is rapidly evolving to meet the ever-changing threat landscape.

As the complexity of corporate networks has grown, so has the sophistication of cyber attacks. Recent trends suggest a move by criminals away from targeted attacks on large-scale information processers – with the intention to steal trade secrets, credit card numbers and personally identifiable information – toward attacks designed to create disruption in the physical world.

Business supply chains have become a multifaceted and interconnected web of software developers, cloud computing providers, outsourced operations, component manufacturers, raw material suppliers and a plethora of other downstream clients and vendors. Ensuring the control and security of the supply chain has become a matter of ever-increasing significance, with failures capable of crippling business operations – be it an automotive manufacturer reliant on inventory management and just-in-time production, or an application provider dependent on an outsourced cloud solution.

As evidence of this diversification of approach by malicious actors, surveys show that 48 percent of UK manufacturers have been subject to a cyber security incident[1], with half of them suffering financial loss or disruption to business as a result.

These core business operations rely on industrial control systems, which can be broken down into three main groups: Programmable Logic Controllers (PLCs); Systems Control and Data Acquisition (SCADA); and Distributed Control Systems (DCS). These systems have become a focus of recent attacks involving 'CrashOverride' – a malware targeting electrical grid operations which caused a Ukrainian power outage – and 'Trisis', a malware targeted at control units dedicated to safety[2]. Given the highly disruptive capability of these attacks, activity in the Industrial Control System space is only set to increase.

The potential impact has been demonstrated through the multi-million dollar losses suffered by Maersk, TNT Express and Mondelēz, just to name a few, the root cause of which was Not-Petya, an encryption ransomware that exploited vulnerabilities in accounting software used by many multinational organizations to process tax payments for their Ukrainian subsidiaries. Banks, airports, manufacturers and logistic companies across the world were paralysed as a result[3]. In another instance, a software vulnerability in a popular utility tool, CCleaner[4], was exploited to spread malware to more than two million PC users. In a separate case, hackable chips were also implanted into devices and systems via Supermicro production facilities, which ultimately affected the servers of 30 U.S. companies. The examples are numerous and growing in frequency.

Supply chain exploits have traditionally involved software attacks carried out by malicious actors attempting to access a network through third parties' connections to it. However, hardware vulnerabilities being exploited and motherboards and micro-chips becoming a stealth doorway into companies' networks is a more recent trend. The recent Supermicro exploit[5], combined with the fallout of the Spectre and Meltdown hardware vulnerabilities, demonstrates the potential for systemic hardware issues to materially impact the supply chain and physical capabilities of any business.

The cyber insurance market has already taken important steps to address these exposures by helping insureds protect themselves against supply chain risk. Clients are increasingly seeking the extension of Business Interruption cover to include events that occur at third-party IT vendors, resulting in a loss of income and additional expenses incurred to mitigate the impact. A recent challenge has been requests to expand this cover to include non-IT vendors. This opens insurers up to claims arising from a failure of IT infrastructure occurring at the premises of any of its suppliers, regardless of the type of service or product delivered. This is a material exposure which is almost impossible to underwrite adequately.

With the absence of information and lack of direct oversight over third-party controls and procedures, it is as difficult for businesses to protect themselves from third-party risk as it is for underwriters to assess the exposure. However, there are key practices underwriters can look for when considering supply chain exposure within a business and the potential loss scenarios emanating from them. These include businesses conducting appropriate due diligence and vendor audits and ensuring that their security controls are of an equivalent level or exceed that of the insured's. Underwriters can also look for assurances that the insured limits vendors' network access to what is needed for critical business operations, ideally with vendors operating on a segregated part of the network and using a multi-factor authentication method. Securing against hardware vulnerabilities within industrial control units can be more difficult given the fact that systems tend to be older (and therefore harder to patch), have a broader attack surface, are less standardised and are generally not designed to operate in a highly connected environment. As such, businesses should have a good understanding of the risks and consequences before integrating these historically air-gapped systems into an interconnected network.

When transferring these risks to the insurance market, additional complexities must be considered. For example, there is often an overlap between standalone cyber policies and other insurance lines – particularly property and casualty – where, in the absence of a specific cyber exclusion, there is debate over whether cyber cover is provided – so called 'silent' or non-affirmative cyber. This can cause confusion in how different policies will respond and may delay the mitigation and settlement of claims as a result. This situation arose in a recent incident involving a large pharmaceutical company, where, parallel to the cyber policy, there was a property programme in place that did not exclude business interruption coverage relating to a cyber event[6].

Confusion surrounding this issue can materially affect the size of a potential claim given the urgency for response and mitigation demanded by a cyber event. Most cyber policies offer a panel of breach response and forensics firms, which the insured can call upon to mitigate potential breach events. Clients should look for insurers that provide direct access to industry-leading breach consultation and PR expertise to help mitigate further damage to their brand. It is always preferable for the insured to call an expert for advice for a non-event rather than have it go unresolved and grow into a material loss and cause significant damage to their reputation, which is then difficult to recover from and rebuild.

As businesses continue to adapt to the ever-increasing complexities of supply chain exposure and the evolving threat landscape, the insurance market is stepping in to ensure peace of mind and clarity of coverage in a world of increasingly intangible risk. However, brokers have to work hard to ensure the overlap of coverage is analysed and discussed thoroughly at the placement stage, both with clients and underwriters, in order to prevent unintended gaps in coverage and ensure the interaction of different policies does not become an after-thought in the event of a serious issue. •

Mauro Signorelli

Joined Aspen Insurance in February 2017 and is a Senior Underwriter in the Aspen Insurance Global Tech E&O and Cyber team. Based in London, he focuses on the growth of the international cyber portfolio by writing large and complex risks. He has extensive experience as an underwriter in international technology and cyber having insured some of the largest European corporations.
Before joining Aspen Insurance, Mauro spent five years at XL Catlin leading the development of their European strategy in the space. Prior to that, he worked for AIG and trained at Simmons & Simmons as a lawyer.
Having worked in Milan, Paris and London he has an in-depth knowledge of the European market and is fluent in Italian and Spanish.
Mauro has a Masters in Law and maintains a Certified Information Privacy Technologist (CIPT) designation.

1. www.computerweekly.com/news/252439718/Nearly-half-of-UK-manufacturers-hit-by-cyber-attacks
2. www.computerweekly.com/news/252436129/Cyber-threat-to-industrial-control-systems-highest-yet
3. www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world
4. www.thehackernews.com/2018/04/ccleaner-malware-attack.html
5. www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
6. www.mobile.royalgazette.com/re-insurance/article/20170915/insurers-grappling-with-scale-of-cyber-risk&template=mobileart