LOCKTON
UNCOMMONLY INDEPENDENT

State-Sponsored Attacks and Cyber Insurance Implications

In March 2020, hackers believed to be operating on behalf of a foreign government infiltrated software provider SolarWinds and then deployed a malware-infected update for its Orion software to infect numerous government and company networks. Full details are available here.

It appears that the goal of the attackers was not to compromise SolarWinds per se but to use the software provider and its software update as a Trojan Horse for access into their customers' networks. From March through to June 2020 any customer that downloaded the software update also received the malware from the attackers: it is reported that nearly 18,000 customers of SolarWinds received the updates.

Not all customers who received the malware have seen it used for attacks. However, it has been used against some strategically critical and sensitive US organisations such as the US Treasury Department, the US Department of Commerce's National Telecommunications and Information Administration (NTIA), the Department of Health's National Institutes of Health (NIH), the Cybersecurity and Infrastructure Agency (CISA), the Department of Homeland Security (DHS), and the US Department of State, as well as commercial companies such as FireEye.

The ultimate objective of the attackers appears to have been to gain information and intelligence (including commercial secrets), and in some cases to steal proprietary code.

Notwithstanding what appears to be a focus on significant strategic US organisations, it is clear that the threat remains for all infected business networks. Once the Trojan Horse malware reaches a customer's network, significant damage can be done. On this basis, SolarWinds has issued emergency patches and urged all its customers to implement them as soon as possible. If an organisation uses SolarWinds software, or if its IT service providers use it, a full forensic security review is recommended to ensure the attackers have not compromised the network.

Insurance Implications

Cyber Insurance

The SolarWinds cyber-attack brings the vulnerability of businesses into sharp focus. For a start, the supply chain nature of this attack highlights the sheer number of organisations that may typically be affected in assaults of this nature. Secondly, the intrusive nature of the attack itself has the potential to expose organisations' intellectual property, data and other confidential information, thereby leaving them exposed.

This is a timely reminder of the need to consider cyber insurance as part of any cyber hygiene /cyber risk programme, and to review policy limits for those organisations which already have cyber cover in place.

It should be noted that there is no such thing as a standard cyber policy. However, a market-leading cyber insurance policy ought to respond to both first party and third party (liability) costs involved in the fallout from a network attack such as SolarWinds.

A consideration of the need for cyber insurance includes a consideration of policy wording. Particular attention should always be given to exclusions and other clauses in any cyber policy to ensure that cover is not detrimentally affected.

War Exclusions

War exclusion clauses have received a lot of airtime in cyber insurance circles over the past few years. A typical war exclusion would preclude cover for any claim arising out of war or warlike action.

The trigger for this focused attention was the NotPetya ransomware attack which, it is alleged, was carried out by Russia. Some insurers have since argued that such an attack was "an act of war" thereby invoking a war exclusion clause, and attempting to avoid coverage. (It is worthwhile noting that this argument was run by insurers of other lines of insurance, not on cyber policies).

For some time London cyber markets have been looking to clarify the war exclusions in cyber policies, particularly in light of increased fears of state-sponsored attacks.

The Geneva Association has even proposed a new cyber term of "hostile cyber activity" to define state-sponsored cyber operations which do not amount to war itself. The intent is to characterise the war environment into various "states" of war and then work with stakeholders towards accepted definitions of what should and should not be covered by cyber markets. The complexities involved with categorisation are plentiful.

No clear pathway has been agreed upon as yet and there is still some consternation at the uncertainty. Until the London cyber markets reach a landing on this issue, careful consideration must be had to any war exclusion clauses in policy documents. A market-leading policy should include a broad cyber-terrorism carve-back.

(Interestingly, commentators have suggested that the SolarWinds attack, rather than an act of war, was an act of cyber espionage: an accepted practice in peacetime. Certainly the fact that the cyber-attack existed outside any armed conflict, would support this proposition).

SolarWinds Exclusions

We are aware that some markets have been including specific SolarWinds exclusions on policy wordings. There will be instances where a blanket exclusion is not appropriate and broker input will be required to negotiate the best outcome for the insured.

For further information, please contact Lucy Scott or Peter Erceg.

Lucy Scott
T: +44 020 7933 2382
E: lucy.scott@uk.lockton.com

Peter Erceg
T: +44 020 7933 2608
E: peter.erceg@uk.lockton.com

The Lockton Global, Cyber and Technology team works with clients to help protect their business from cyber risks, from ransomware *to phishing, targeted hacks, malware, IP theft and various cyber complexities. Due to the sensitive and confidential nature of such risks, we may have created fictional case studies to demonstrate examples of cyber complexities a client might experience. The case studies are inspired by real matters, however, some facts may have been amended to protect client confidentiality. These case studies do not constitute advice. Please seek appropriate advice before taking any action.*

LOCKTON
UNCOMMONLY INDEPENDENT